



# **BISHOP FOX**

# **CYBERSECURITY STYLE GUIDE**

VERSION 1  
FEBRUARY 15, 2018



**Bishop Fox Contact Information:**

+1 (480) 621-8967

[style@bishopfox.com](mailto:style@bishopfox.com)

8240 S. Kyrene Road

Suite A-113

Tempe, AZ 85284

**Contributing Technical Editors:**

Brianne Hughes, Erin Kozak, Lindsay Lelivelt, Catherine Lu

We want to thank all of our Bishop Fox consultants, especially Dan Petro, for reviewing and improving the guide's technical content.

---

# TABLE OF CONTENTS

<b>Welcome!</b> .....	<b>4</b>
Technical Formatting .....	5
What to Expect in the Guide .....	6
<b>The Cybersecurity Style Guide</b> .....	<b>7</b>
A-Z.....	7
<b>Appendix A: Decision-making Notes</b> .....	<b>86</b>
How We Choose Our Terms .....	86
How To Codify Your Own Terms .....	87
<b>Appendix B: External Resources</b> .....	<b>88</b>
<b>Epilogue</b> .....	<b>92</b>

---

# WELCOME!

We are Bishop Fox, a global information security consulting firm based in the United States. Welcome to our cybersecurity style guide. We compiled this guide to keep ourselves technically accurate and up to date in our reports, presentations, and social media interactions. Now we want to share this version of our standards with you.

This guide is designed for security researchers. It provides advice on which words to use in reports, how they should look in the middle of a sentence, and how to pronounce them out loud. Since the terms are listed alphabetically, you'll find serious usage advice right next to playful entries about internet culture.

Each term in the guide earned its place by being unintuitive in some way:

- It may look like a non-technical word ([execute](#), [pickling](#), [shell](#)),
- It may be uniquely written ([BeEF](#), [LaTeX](#), [RESTful](#)),
- It may not follow a clear pattern ([web page](#) vs. [website](#)),
- It may have a very specific technical distinction ([invalidated](#) vs. [unvalidated](#)),
- Or its meaning may change depending on the context ([crypto](#), [PoC](#), [red teaming](#)).

Language is always evolving, and those changes are especially visible in an innovative field like information security. This guide aspires to record those changes in vocabulary and encourage researchers to use language intentionally as the digital lexicon continues to grow. Learn more about what guides our style choices in [Appendix A](#).

This is a work in progress. We intend to revise this list in the future and share subsequent versions with the public. Please contact [style@bishopfox.com](mailto:style@bishopfox.com) with ideas about new entries or improvements to existing entries.

---

## NOTE

This guide is a starting point for further research into technical terms, not a comprehensive dictionary. We provide usage notes about capitalization, fonts, and pronunciation where needed, but not every term here is defined. External resources with detailed technical definitions can be found in [Appendix B](#).

# Technical Formatting

We use two fonts. Most of our text appears in Open Sans (this sans serif font). We refer to Open Sans in the style guide as the **normal font**. The secondary font is Source Code Pro, a monospace (fixed-width) font that we refer to throughout this guide as the **tech font**.

The tech font makes technical terms stand out to the reader when they appear in and out of quoted code. We use the tech font for several reasons in several ways. Even with the chart below, we're still finding gray areas. Here is an overview of how we use these fonts:

Normal Font	Tech Font
Titles of documents and file types <code>Bishop Fox Security Style Guide, a PDF file</code>	Full names of documents and files <code>Security_Style_Guide.pdf</code>
Error messages and security questions <code>"Please enter a valid user ID."</code>	File paths <code>server/web/directory/</code>
Names of organizations, companies, and teams <code>DEF CON, .NET, Tor, assessment team</code>	Email addresses <code>style@bishopfox.com</code>
Names of products and their versions <code>Ethernet, Steam, Ubuntu 17.04</code>	Username and passwords <code>@bishopfox, admin:admin, password</code>
Types of requests <code>GET request, pull request, PUT request</code>	URIs and URLs <code>data:, www.bishopfox.com/[variable]</code>
Ports by themselves <code>port 80, port 443</code>	IP addresses (with or without ports) <code>192.168.1.1, 192.168.1.1:80</code>
Types of fields, headers, parameters, etc. <code>data element, content-type header</code>	Names of fields, headers, parameters, etc. <code>C: drive, Secure flag, url parameter</code>
Line numbers <code>"On line 42 of the code excerpt..."</code>	Quoted code <code>"Block [\n] and [?] characters"</code>
Vulnerability IDs <code>CVE-2014-6271, MS15-034, RFC 1918</code>	Code excerpts <code>&lt;b&gt;Hello World!&lt;/b&gt; 3. Go to 1</code>

Terms that use the tech font appear in that style no matter where they show up in a report, including bullet points and figure captions.

## Bold Text

When writing about clickable buttons in reports, we follow the Microsoft Manual of Style (see Appendix B). We bold button names that the reader is meant to click. When writing about a feature with the same name as a button, capitalize it if applicable, but don't bold it.

- Click **Track Changes** to show all your future changes in Word.
- The Track Changes feature allows users to track their edits.
- After hitting the **OK** button, the user was redirected to the Home tab.

Within the style guide word list, bolding indicates that a related term has its own entry.

## What to Expect in the Guide

Each headword appears in either normal or tech font and is capitalized as it would appear in the middle of a sentence. For example:

### **denial of service** (n.), **denial-of-service** (adj.) (**DoS**)

A [denial of service](#) is caused by [denial-of-service](#) attacks. Spell out on first use. DoS is pronounced as “doss” or spoken as the whole phrase, not the acronym.

Related: **DDoS**

Some entry headings clarify parts of speech: [\(adj.\)](#) for adjective, [\(n.\)](#) for noun, [\(v.\)](#) for verb.

Many security terms have disputed pronunciations because they were typed first and then spoken out loud later. Pronunciation is provided for select terms in the guide. Be aware that some acronyms look similar but are pronounced differently:

[CIO](#) is pronounced as letters, but [CISO](#) is pronounced as “seeso.”

[UI](#) is pronounced as letters, but [GUI](#) is pronounced as “gooey.”

[PoC](#) is pronounced as letters, but [T-POC](#) is pronounced as “tee-pock.”

[OSINT](#) is pronounced “O-S-int” but [OWASP](#) is pronounced “oh-wasp.”

By combining the use of two fonts, button bolding, and the big word list below, we strive to be accurate, consistent, and understandable to our clients. It's been helping us internally and we hope it helps you now, too.

---

# THE CYBERSECURITY STYLE GUIDE

## A-Z

!

The exclamation point or bang.

@

The at sign.

Related: **email, handle, username**

#

The pound sign or hashtag. Only called hashtag when tagging something. This character and [#] are sometimes used interchangeably and are pronounced as “sharp” in programming language names.

Related: **C#, characters, numbers, tweet**

/

Slash. Avoid using the slash to compare two things outside of set phrases like 24/7, and/or, client/server, h/t, and TCP/IP.

Related: **mm/dd/yyyy, s/o, SSL/TLS**

\

Backslash.

'

Tic character. Not an apostrophe.

### **0-day** (n. or adj.)

A “zero-day” or “oh-day” finding. In formal writing, it’s better to use [zero-day finding](#), [previously undisclosed vulnerability](#), or [publicly undisclosed vulnerability](#).

### **2FA or TFA**

Two-factor authentication.

Related: **MFA**

### **3DES**

Triple DES. A symmetric key block cipher. DES is pronounced as letters or “dez.”

### **3D printing**

### **3G, 4G**

Third- and fourth-generation communications technology. Cell phone network options. Do not spell out.

Related: **CDMA, GSM**

### **3Scale**

An API management platform.

### **4chan**

A website for trolls and memes that birthed Anonymous and rickrolling.

Related: **dox, message board, NSFW, troll**

### **7-Zip**

An open source file archiver.

### **8.3 filename**

Related: **short-name**

### **8-bit** (adj.)

### **2600**

A hacker magazine founded in 1984. Also a series of local clubs. <https://www.2600.com/>

# A

## **a vs. an**

Use “an” when the next word begins with a vowel sound when spoken, regardless of spelling. [A](#) hybrid test. [A](#) unified problem. [A](#) Xerox machine. [An](#) HTTP issue. [An](#) SSH tunnel. [An](#) underlying cause. [An](#) XSS attack.

## **a11y**

Accessibility, often in relation to technology. 11 represents the 11 letters removed from the middle of the word.  
Related: [i18n](#), [L10n](#), [k8s](#)

## **abort (v.)**

Avoid using the verb unless it's in quoted code. Try [force quit](#) or [interrupt](#) instead.

## **abuse (n.)**

This is acceptable in common industry phrases like “application abuse.” Avoid using it on its own if possible. Try “malicious use or usage” instead.

## **abuse (v.)**

OK in set phrases but do not use it on its own. Try [alter](#), [automate](#), [compromise](#), [deface](#), [exhaust](#), [exploit](#), [force](#), [impersonate](#), [manipulate](#), [misuse](#), [reuse indefinitely](#), [take advantage of](#), or a more specific verb instead.

## **-accessible (adj.)**

Always hyphenate.

## **access point (AP)**

Spell out on first use.

## **ACE**

Arbitrary code execution. Spell out on first use.

## **ACL, ACLs**

Access control list. Spell out on first use.

## **AD**

Active directory. Spell out on first use.

## **adb or adb**

Also called the Android debugger, adb is both a command and a technology for interacting with an Android phone connected to a computer.

## **ad blocking (n.), ad-blocking (adj.)**

## **add on (v.), add-on (n.)**

## **address bar**

## **ad hoc (adj.)**

Describes immature security infrastructure. In networks (especially wireless ones), ad hoc means decentralized.

## **admin or admin**

Short for administrator. Write in normal text if referring to the role or admin privileges. If referring to the username `admin`, use tech font.

## **adversary**

Do not use this term in formal writing; use [attacker](#) or [malicious user](#) instead.

**AES**

Advanced Encryption Standard. Spell out on first use.

**Agile process**

Related: **scrum, sprint**

**AI**

Artificial intelligence, often used as jargon to refer to a computer program. AI can also mean Amnesty International.

Related: **Deep Blue, HAL 9000, machine learning, replicants, The Three Laws of Robotics, Turing Test, Watson, WOPR**

**Airbnb****air-gapped** (adj.)

Air-gapped systems are disconnected from insecure networks and the internet.

**Akana**

An API management provider.

**alert box****Alexa**

Amazon AI.

Related: **Cortana, Google Assistant, Siri**

**algorithm** (n.)**alphanumeric** (adj.)

Describes strings that contain letters and numbers, not special characters, punctuation, or spaces.

**a.m.**

Put a space after the number as in “4 a.m. GMT.” Include the time zone if referring to a testing window or specific event.

**Amazon EC2, Amazon ECR, Amazon RDS**

Web services. After first use, you can refer to the services by name without “Amazon.”

**analog****and/or**

Use sparingly in formal writing.

**Android**

Google’s mobile operating system.

**android** (n.)**angle brackets**

The < and > characters.

Related: **characters**

**AngularJS**

A JavaScript framework.

**Animoji**

Animated emoji created by Apple.

**anonymization****Anonymous**

International group of 4chan hackers with a Guy Fawkes mask symbol.

**anti-malware****antivirus (AV)****Apache Server**

## **Aperture Science**

A fictional research company from the Portal series of video games.

## **API, APIs**

Short for application programming interface. How software interacts with other software. Do not spell out.

## **app vs. application**

Smart devices like phones and tablets have apps, computers have applications. App can also be a shortened form of application. To the security industry, they are all computer programs.

## **Apple**

Related: **FaceTime, FairPlay, iOS, iPhone, Lightning cables, MAC OSX, macOS-based, PowerBook, Siri**

## **applet (n.)**

## **Apple TV**

## **application security**

Alternate term for information security.

## **APT**

Short for application penetration testing. Also stands for advanced persistent threat or advanced packaging tool. Spell out on first use in public-facing documents. Related: **criticality, EPT, IPT, pen testing**

## **AR**

Augmented reality. Related: **IoT, VR, Vuforia**

## **arbitrary (adj.)**

Of the attacker's choosing, as in "the user would be redirected to an arbitrary URL."

## **Archer**

An animated spy TV show that inspired the name of the Bishop Fox Danger Drone. It's also the name of an RSA security product.

## **Arduino (n.)**

Pronounced "ar-dweeno."

## **ARM**

Short for Architecture Reference Manual or it can refer to RISC architecture used in microprocessors. Define briefly on first use to clarify your intended meaning.

## **artificial intelligence (AI)**

## **ASCII**

Pronounced "ask-ee."

## **ASLR**

Address space layout randomization. Spell out on first use.

## **ASP.NET**

## **asset**

Assets are systems, software, applications, libraries, personnel, equipment, or anything else that clients value and want to protect.

## **ASV**

Approved scanning vendors. Spell out on first use. Related: **PCI**

## **ATM**

Short for automated teller machine or “at the moment.” “ATM machine” is redundant.

Related: **PIN**, **SSN**

## **at-rest (adj.), at rest**

[At-rest](#) encryption. Data [at rest](#).

## **attack chain**

Related: **elevation of privileges**

## **attacker-controlled (adj.)**

## **attacker-owned (adj.)**

## **attack surface (n.)**

## **attribute**

A specification of a value. When writing about a type of attribute, use normal font. When discussing a specific attribute, use tech font as in “a username attribute.”

## **audio conference, audio conferencing**

Related: **videoconferencing**

## **audit trails**

## **AUP**

Acceptable Use Policy. Spell out on first use.

## **authentication**

## **authorization bypass**

## **autocomplete (n. or v.)**

A generic term for an application feature that predicts the rest of the word or phrase as a user types.

## **autocorrect (n. or v.)**

A generic term for an application feature that fixes identified mistakes in typed words.

## **autofill**

## **automation**

The automatic operation of required processes.

## **auto-renew (v.)**

## **avatar**

## **AWS**

Amazon Web Services.

# **B**

## **backdoor (n. or v.)**

## **back end (n.), back-end (adj.)**

## **backported (adj.), backporting (n. or v.)**

## **backslash** or \

## **backtrace**

Related: **traceback**

## **back up (v.), backup (n. or adj.)**

## **backwards compatibility (n.)**

## **backwards compatible (adj.)**

**badput**

Related: **goodput**, **throughput**

**bandwidth**

The speed of a data network. "Never underestimate the bandwidth of a station wagon full of tapes hurtling down the highway." – Andrew Tanenbaum

**bank drops****barcode****bar mitzvah attack**

An SSL vulnerability. So named because its security implications were realized 13 years after it first appeared in the codebase.

**Base64-encoded** (adj.),**Base64 encoding** (n.)**-based** (adj.)

Always hyphenate.

Ex: [host-based](#), [logic-based](#), [role-based](#)

**baseline****Bash****BASIC**

A programming language.

**bastion host**

A specially hardened host often used as a gateway to pivot into other hosts.

**BBS**

Bulletin board system.

**BCC, BCC'd, BCCing**

Blind carbon copy. Do not spell out.

Related: **CC**, **email**

**BCP**

Business continuity plan. Spell out on first use.

**bcrypt**

Pronounced "bee-crypt." A password hashing function.

**BEC**

Business email compromise. Spell out on first use.

Related: **phishing**

**BeEF, BeEF hooking**

Browser Exploitation Framework.

**BER**

Bit error rate. Spell out on first use.

**best practices**

Business jargon, use sparingly. Practices that align with compliance guidelines or industry standards.

Related: **CIS 20**

**beta** (n. or adj.)**BF**

An informal name for Bishop Fox. Used very sparingly in places where space is limited.

**BGP**

Border Gateway Protocol. Spell out on first use.

## **Big Brother**

The symbol of totalitarian surveillance from the novel Nineteen Eighty-Four. Big Brother is watching you.

## **big data**

## **big-endian** (adj.)

## **BIG-IP**

A load balancer. Pronounced “big-eye-pee.”

## **billion laughs attack**

Related: **DoS**

## **binary**

Base-2 number system. 0 or 1. Can also refer to binary executable files.

Related: **big-endian, little-endian**

## **BIND**

A DNS server.

## **birds of a feather (BoF)**

An informal discussion group.

## **birth date**

## **Bishop Fox**

Our company.

Related: **foxes, Lucius Fox, Martin Bishop**

## **bit** (n.), **-bit** (adj.)

As in “a key length of at least 2048 bits” or “a 2048-bit RSA key.” When abbreviated, use lowercase **b** for bits, uppercase **B** for bytes.

## **Bitbucket**

An Atlassian product for Git.

## **bitcoin**

Digital cryptocurrency.

Related: **coins vs. tokens, cold wallet, hot wallet, securities**

## **bit-flipped** (adj.), **bit-flipping** (adj.)

## **BitLocker**

Microsoft Windows disk encryption software.

## **bitstream**

## **BitTorrent**

## **BlackBerry**

## **black-box testing**

## **Black Hat**

A series of annual security conferences that happen in the USA, Europe, and Asia.

<https://www.blackhat.com/>

## **black hat**

An attacker or malicious user.

## **blacklist** (v. or n.), **blacklisting**

Related: **blocklist**

## **black market**

We prefer this term in formal reports to describe unindexed illegal online activity hubs. Tor and I2P are colloquially known as “dark web” browsers.

Related: **fullz, I2P, Tor**

## **bleeding edge** (n. or adj.)

**blind** (adj.)

During a blind attack, the attacker is unable to view the outcome of an action.

**bloatware****BLOB** or **blob**

Binary large object.

**blockchain, block chaining**

Related: **CBC, cryptocurrency**

**blocklist, blocklisting**

A proposed alternative term for blacklisting.

Not yet widespread.

Related: **safelist**

**blog, blogroll****Bloodhound**

A pen testing tool.

**Blowfish**

An encryption algorithm.

**blue screen** (v.)**Blue Screen of Death (BSOD)****blue team, blue teaming** (v.)

Blue teams run scenarios to defend a target or environment from potential attackers.

They reduce the attack surface, employ hardening strategies, and use honeypots.

Related: **red team, purple team**

**Bluetooth**

A unifying wireless system named after a Norwegian king, Harald Bluetooth.

**Blu-ray****BMP file, .bmp file**

Short for bitmap.

**Bomgar**

An IT support portal.

**Boolean operators**

Useful AND precise.

**boot chain** (n.)

Related: **start up**

**boot time** (n.)**Boston Dynamics****bot**

An automated program like a chatbot or Twitterbot.

**botnet**

A network of bots sometimes used in ransomware attacks.

**Brainfuck**

An esoteric programming language.

**breadcrumbs, breadcrumb trail****breakpoint** (n. or v.)**brick**

Informal. An old heavy cell phone or a dead device.

**brick-and-mortar** (adj.)

Describes IRL places of business.

**browsable** (adj.)**browser fingerprinting**

## **browser hijacking**

**brute-force** (v. or n.), **brute-forcing** (n.)

## **BSD**

Berkeley Software Distribution.  
A Unix-derived operating system.

## **BSides**

A global series of security events.  
<http://www.securitybsides.com/>

## **bucket**

When discussing a type of bucket, use normal font. When discussing a specific bucket by name, use tech font for the name as in "an oz-provision bucket."

## **buffer overflow**

## **bug bounty**

## **Bugcrowd**

A crowdsourced bug bounty security company.

**built-in** (adj.)

**bulleted** (adj.)

**bullet point** (n.)

## **Burp Suite, Burp Collaborator**

A web application proxy.

**business impact analysis (BIA)**

Spell out on first use.

## **BuzzFeed**

## **BYOD**

Bring your own device. Describes companies that allow employees to use their own computers and phones for work.

**bypass** (v. or n.)

## **byproduct**

## **bytes**

Kilobytes, megabytes, gigabytes, terabytes, petabytes. KB, MB, GB, TB, PB. No space between number and unit as in 64TB. Use uppercase **B** for bytes, lowercase **b** for bits.  
Related: **MiB, units of measurement**

# **C**

## **C#**

A programming language. Pronounced as "C sharp."

Related: **#, hashtag**

## **CA**

Certificate or certification authority. Spell out on first use.

Related: CEH, CISSP

**cache** (n. or v.)

**cache busting**

**cache poisoning**

## **CactusCon**

An annual security conference in Arizona.  
<http://www.cactuscon.com/>

**callback** (adj. or n.)

As in “a crafted callback parameter.”

**CAM**

Computer-aided manufacturing. Spell out on first use.

Related: **LMS**

**canary account**

Related: **honeypot**

**canonicalization, canonicalize****CAPTCHA, CAPTCHAs**

The Completely Automated Public Turing test to tell Computers and Humans Apart. A challenge-response test.

Related: **computer vision, reCAPTCHA**

**carriage return character** or `\r`

An invisible character that makes the text go back to the beginning of the line. It’s a skeuomorph that refers to the way typewriters need to “return” a carriage to its original position.

**case-by-case** (adj.)**cash-out guide****catch** (v.)

Related: **throw**

**The Cathedral and the Bazaar (CatB)****CBC**

Cipher block chaining. Spell out on first use.

**CC, CC’d, CCing**

Carbon copy. Do not spell out.

Related: **BCC, email**

**CCC**

Chaos Communication Congress. An annual security conference in Germany.

**CCTV**

Closed circuit television.

**CD, CD-R, CD-ROM, CD-RW****CDMA**

Code division multiple access.

**CDN**

Content delivery network. Spell out on first use.

**CDP**

Clean desk policy. Spell out on first use.

**CEH**

Certified Ethical Hacker.

**cell phone****certificate****CFO**

Chief Financial Officer.

**CGI**

Short for computer-generated images or, less commonly, Common Gateway Interface. Define briefly on first use to clarify your intended meaning.

**challenge-response mechanisms**

Robot-filtering tests like CAPTCHA.

Related: **Turing Test**

**changelog**

## characters

When calling out specific characters (keystrokes) that affect the meaning of a code sequence, use tech font surrounded by square brackets in normal font as in “added a single quote [‘].” If the character’s name is also its symbol, write it in tech font. If the font difference is not visible, use quotation marks as in [30,000 “A” characters](#).  
Related: **metacharacters**, **wildcards**

## chatroom

### chattr

Short for change attribute. Pronounced as “chatter.”  
Related: **chmod**, **chroot**

## checkbox (n.)

## check out (v.), checkout (adj. or n.)

## checksum, checksums

## child abuse material

This is a more accurate term for child pornography. If you discover child abuse material in the context of your work, report it to a manager immediately. If you find it online outside of work, quickly contact NCMEC—The National Center for Missing and Exploited Children.

## chmod

Change mode. Pronounced as “change mod,” “C-H-mod,” or “chuh-mod.”  
Related: **chattr**, **chroot**

## Chrome

Google browser.

## Chromecast

## chroot

Change root. A Unix operation that simulates a directory on a filesystem as if it were the root of the filesystem. Pronounced as “C-H-root” or “chuh-root.”  
Related: **chattr**, **chmod**

## chroot directory or ChrootDirectory

An SSH directory.

## chroot jail

A way to isolate a process from the rest of the system.

## CIA

Short for the Central Intelligence Agency or the triad of information security concerns: confidentiality, integrity, and availability.

## CIO

Chief information officer.  
Related: **CFO**, **CISO**

## cipher

Don’t use “cypher.” Write the names of ciphers in normal font as in Blowfish.  
Related: **RSA**, **SHA**

## cipher suite

## ciphertxts

## CIS 20

The Center for Internet Security has a list of 20 guidelines for securing organizations.  
<https://www.cisecurity.org/controls/>

## Cisco

**CIS CSC**

CIS Critical Security Controls.  
Related: **CIS 20**

**CISO**

Chief Information Security Officer.  
Pronounced "seeso."

**CISSP**

A security certification. Certified  
Information Security Systems Professional.

**class**

When discussing a specific class by name,  
use tech font as in "a Time class."

**cleartext vs. plaintext**

In common usage, these terms are used  
interchangeably. In our reports, [cleartext](#)  
means unencrypted content. [Plaintext](#) is a  
more technical term that describes the  
input to a cryptographic system (which itself  
may already be encrypted or hashed).  
Related: **CPA**

**clear web or Clear Web**

This is used in contrast to the "dark web" or  
"dark net" parts of the internet. It refers  
vaguely to publicly accessible sites that  
have been indexed by search engines.  
Do not use in formal writing.

**CLI**

Short for command-line interface or  
command language interpreter. Spell out  
on first use.

**clickbait****clickjacking**

In formal writing, we refer to this finding as  
"user interface (UI) redress." It's also called  
"cross-frame scripting."

**click through (v.)****clickthrough (adj. or n.)****client-side (adj.)****clip art****Clippy**

Discontinued anthropomorphic paper clip  
assistant in Microsoft Office.

**closed caption (n.), closed-caption (adj.)****the cloud**

Business jargon. "The cloud" is just servers.

**cloud computing****CloudFront**

An AWS content delivery network (CDN).

**CloudTrail**

An AWS logging and monitoring service.

**cluster (n.)**

As in "provision a cluster on each account."

**CMDB**

Content management database. Spell out  
on first use.

**CMS**

Content management system. Spell out on  
first use.

**co-creator****code** (n. or v.)**codebase**Related: **user base****codec**

Code/decode.

**Codecademy****code path****code shrinking****coins vs. tokens**

These are units of worth in virtual currencies. These terms are sometimes used interchangeably and sometimes used very differently. Define briefly on first use to clarify your intended meaning.

Related: **bitcoin, cryptocurrency****cold-call** (v.) **cold call** (n.)

A social engineering strategy.

**cold storage** (n.)**cold wallet**

Offline bitcoin storage.

Related: **hot wallet****command and control (C2) machine****command line** (n.), **command-line** (adj.)**commercial-free** (adj.)**commodity hardware**

Over-the-counter hacking tools that anyone could get and use.

**company-wide** (adj.)**compensating controls****compile** (v.)**compliance framework****computer vision** (n.)**configuration drift****connect-back shell** (n.)**constants** (n.)

Pre-defined variables that are referenced in later code.

**containerization****content injection****content spoofing****content type, Content-type header****-controlled** (adj.)

Always hyphenate.

Ex: [attacker-controlled](#), [user-controlled](#)**cookie** (n.)**cookie poisoning, cookie security****cooperate** (v.)**coordinate** (v.)

**copycat** (adj. or v.)

Related: **spoof**

**corrupted** (adj.)

**CORS**

Cross-origin resource sharing. Spell out on first use.

**Cortana**

Microsoft AI.

Related: **Alexa, Google Assistant, Siri**

**countermeasure** (n.)

**coworking space**

**CPA**

Chosen-plaintext attack. Spell out on first use.

**CPU**

Central processing unit. Do not spell out.

**crack** (v.)

**crawl** (v.)

**credential reuse** (n.)

**credentials** (n.)

The information necessary to pass a security check—often a username and password. Sometimes an RFID badge.

**critical** (adj.)

Describes a non-negotiable business function or a vulnerability with catastrophic consequences that is easily exploitable.

**criticality**

A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

**cron**

Cron is a utility.

**cron job** (n.)

**cross-platform** (adj.)

**cross-site scripting (XSS)**

There are three kinds of XSS: reflected, stored, and DOM-based.

**Crowbar**

A password-cracking tool.

**crowdfund** (v.)

**crowdsource** (v.), **crowdsourcing** (n.)

**CRUD**

Create, read, update, destroy.

**cryptanalysis** (n.), **cryptanalytic** (adj.)

**crypto**

Historically, this was short for cryptography. Now, it can also mean cryptocurrency. Spell out on first use to clarify your intended meaning.

**cryptocurrency**

Virtual currency.

Related: **bitcoin, blockchain, coins** vs.

**tokens, salami slicing attack, securities**

**cryptographically**

**CSP**

Short for Content Security Policy. Spell out on first use.

**CSPRNG**

Short for Cryptographically Secure Pseudo-Random Number Generator. A secure way of generating random numbers. Spell out on first use.

**CSRF**

Short for cross-site request forgery. A common vulnerability. Spell out on first use.

**CSS**

The HTML cascading style sheets feature. Do not spell out.

**C-suite** (adj. or n.)

High-level executives like CEOs and CIOs.

**CSV file, .csv file**

Comma-separated value(s).

**CSWSH**

The cross-site WebSocket hijacking vuln. Spell out on first use.

**CTF**

Capture the flag. Spell out on first use in public-facing documents.

**CTO**

Chief Technology Officer.

**CTR**

Short for clickthrough rate or Counter Mode. Spell out on first use.

**Cupertino effect**

An error in early Apple dictionaries that corrected “cooperation” to “Cupertino” because of their limited word list.

**cURL**

Pronounced “curl.”  
Related: **Wget**

**currency**

Our reports rarely include specific values but we default to USD as in \$1.50. Follow AP style for mixed currency situations.

**cursor** (n.)**custom-written** (adj.)**cutting edge** (n.), **cutting-edge** (adj.)

Related: **bleeding edge**

**CVE**

Common Vulnerabilities and Exposures. A system that catalogs publicly known vulnerabilities and exposures. CVE references are written in normal font as in [CVE-2014-6271](#).

**CVSS**

Common Vulnerability Scoring System. Spell out on first use.

**CW**

Content warning.

**CWE**

Common Weakness Enumeration. Write weaknesses in normal font as in [CWE-565](#).  
Related: **CVE**

## **cyber-**

Industry professionals don't use this prefix, but it's helpful when informing the public, as in the title of this document. For many users, "cyber" on its own invokes cybersex, not hacking. <https://willusingtheprefixcybermakemelooklikeanidiot.com/>

Related: **cybersecurity**

## **cyberpunk**

A subgenre of science fiction.

## **cybersecurity**

Defense contractors and government officials use this term or "infosec." Industry professionals do not prefer this term, but it is used for clarity with the public, as in the title of this document. We prefer the term [information security](#).

Related: **cyber-**, **infosec**

## **cyborg**

A hybrid organic being. Coined in 1960 to mean cybernetic organism.

## **Cycript**

A reverse engineering tool for iOS devices.

## **Cydia**

An app found on jailbroken iOS devices.

## **Cylon**

Fictional cyborgs in Battlestar Galactica.

# **D**

## **daemon**

Pronounced as "demon." Describes a background system process on a computer.

## **Danger Drone**

A Bishop Fox creation. It's a Raspberry Pi on a drone that can access tall buildings inconspicuously as a flying hacker laptop.

## **DAO**

Short for decentralized autonomous organization or Data Access Object. Spell out on first use.

## **dark net or Dark Net**

This nebulous term, along with "dark web" and "deep web," are written and used inconsistently to refer to online black markets. Better to call it the black market or specify the site or service in formal writing.

Related: **Tor**, **I2P**

## **Dark Reading**

A security industry publication.

## **DARPA**

Defense Advanced Research Projects Agency.

## **data**

Always write data in the singular as in "the data was recovered."

## **data://**

Use tech font for data URIs.

**database**

**data center**

**data files**

**data handling** (adj. and n.)

**data-only** (adj.)

**dates**

Be aware of possible day/month confusion with global audiences.

Related: **mm/dd/yy**

**datetime**

**day-to-day** (adj.)

As in “day-to-day activities.”

**DB**

Short for database. Spell out on first use unless it’s part of a larger phrase like Mongo DB or IMDB.

**dba**

Short for “doing business as” or “database administrator.” Spell out on first use in public-facing documents.

**DDE**

Dynamic Data Exchange. Spell out on first use.

**DDoS**

Distributed denial of service. Pronounced “dee-doss” or as letters. Spell out on first use.

Related: **denial of service, DoS**

**dead code**

OK in formal writing.

**dead drops**

**Debian**

A Linux distribution. Pronounced “debb-ean.”

**debuggable** (adj.)

**decap** (v.), **decapped** (adj.)

**declare** (v.)

To tell a program that a function exists before the function has been defined.

**decommmed** (adj. or v.)

Use “decommissioned” in formal writing instead.

**Deep Blue**

Famous IBM chess-playing AI. The name was inspired by the fictional supercomputer Deep Thought in The Hitchhiker’s Guide to the Galaxy books.

**deep dive** (n.), **deep-dive** (v.)

**DeepHack**

2017 Bishop Fox machine-learning AI that can perform SQL injection attacks.

**deface** (v.)

**DEF CON**

An annual security conference in Las Vegas.

<https://www.defcon.org/>

Related: **Black Hat, SomaFM**

## **DEFCON system**

A military alert scale that is set at DEFCON 5 during peacetime and elevates to DEFCON 4 and above during threatening situations.

## **defense in depth (n.), defense-in-depth (adj.)**

If you are interested in [defense in depth](#), employ a [defense-in-depth](#) strategy,

## **DELETE request**

Related: **request**

## **denial of service (n.), denial-of-service (adj.) (DoS)**

A [denial of service](#) is caused by [denial-of-service](#) attacks. Spell out on first use. DoS is pronounced as “doss” or spoken as the whole phrase, not the acronym.

Related: **DDoS**

## **deny any any**

A rule.

## **deprecate (v.)**

In technical documents, this is similar to “depreciate.” Used when hardware or software is considered retired but left in for backwards compatibility; included but unsupported and unofficial.

## **DES**

Short for data encryption standard.  
A symmetric-key encryption cipher.  
Spell out on first use.

## **deserialization**

## **deus ex machina**

Latin for “god from the machine.” A plot device in which an unresolvable problem is conveniently fixed by an unlikely solution.

## **dev**

Informal. A system in development, as opposed to a production (prod) system.

## **DevOps**

Business jargon. Development operations.

Related: **toolchain**

## **DevSecOps**

## **DHS**

Department of Homeland Security.

## **DHTML**

Dynamic HTML. Do not spell out.

## **dialog box**

## **dial up (v.), dial-up (n. or adj.)**

## **dictionary-based attack**

An automated password-guessing attack. Also called a “dictionary attack.”

## **diff (n. or v.)**

A tool that finds the differences between two texts.

## **-Diggity**

A suffix for tools created by Fran Brown.  
Ex: [GoogleDiggity](#), [SearchDiggity](#)

## **digital certificate**

## **dingbat**

## **directives**

If it's a type of directive, use normal font. If it's a names directive, use tech font as in "SetCookies directive."

## **directory**

If it's a type of directory, use normal font. If it's a named directory, use tech font as in "Moss directory."

## **directory traversal**

In formal writing, we refer to this finding as "path traversal."

## **Dirty COW**

Short for Dirty copy-on-write.  
The CVE-2016-5195 vulnerability.

## **disclosed, disclosure**

## **discrepancy**

## **DKIM**

DomainKeys Identified Mail allows messages that originate from a protected domain to be cryptographically signed. Pronounced "D-kim."  
Related: **DMARC, email, SpoofCheck**

## **DLL file, .dll file**

Dynamic-link library.

## **DLP**

Data loss prevention.

## **DMA**

Short for direct memory access. An exploitable hardware feature.

## **DMARC**

Domain-based Message Authentication, Reporting and Conformance allows an organization to inform other mail servers of what should be done when fraudulent mail from the protected domain is received. Pronounced "D-mark."  
Related: **DKIM, SpoofCheck**

## **DMZ**

Short for demilitarized zone. Also known as a perimeter network. It refers to a less-secured portion of a network between external firewalls and the WAN connection.

## **DN**

Short for Distinguished Name in the LDAP API. Spell out on first use.

## **DNS name**

Short for domain name system. Types of records stored in the DNS database include IP addresses, nameservers, SMTP mail exchangers, and Start of Authority (SOA).

## **Docker**

A platform that makes and manages containers.  
Related: **k8s, Kubernetes**

## **DOCTYPE**

## **DoD**

Department of Defense.  
Related: **DARPA**

## **DOE**

Department of Education.  
Related: **FERPA**

**doge**

Shiba inu dog meme. Such disputed pronunciation. Wow.

Related: **lolcat**, **meme**

**DOJ**

Department of Justice.

**DOM**

Document Object Model. Pronounced “dahm.”

**DOM-based** (adj.)**domain, domain name**

Related: **FQDN**, **TLD**

**domain-joined** (adj.)**domain squatting** (n.)**dongle** (n.)

An object that interfaces with a port and sticks out from it, sometimes hanging down a bit (e.g., USB drive or Bluetooth adapter).

**DOS**

Short for Disk Operating System. This is unlikely to come up in our formal writing, but readers may confuse DoS with this.

**DoS**

Short for denial of service, a common vulnerability. Spell out on first use.

Related: **denial of service**, **DDoS**, **LOIC**

**DoS vulnerability**

Names of specific DoS vulnerabilities are written in normal font as in “MS15-034.”

**dot-com bubble****double-click** (v.)**downgrade attack**

The POODLE attack is a downgrade attack.

**downtime** (n.)**downvote** (v.)**dox, doxed** (v.), **doxing** (v. or n.)

The gathering of PII to maliciously target an individual online and IRL.

**DPAPI**

The data protection application programming interface on Windows.

**dpi**

Dots per inch as in “300 dpi.”

Related: **units of measurement**

**DRAC**

Dell Remote Access Control. Spell out on first use.

**drag-and-drop** (adj.), **drag and drop** (v.)**drive**

If it’s a type of drive, use normal font. If discussing a drive by name, use tech font as in “the C: drive.”

**-driven** (adj.)

Always hyphenate as in “server-driven.”

**DRM**

Digital rights management. Spell out on first use.

**Dropbox**

A file-hosting service.

**drop down** (v.), **drop-down** (n. or adj.)

### **DROWN attack**

Short for Decrypting RSA with Obsolete and Weakened eNcryption. A TLS bug.

### **Drupal**

### **DTD**

Document type definition. Spell out on first use.

Related: **DOCTYPE**

### **DuckDuckGo**

A search engine that doesn't record search histories.

### **dump** (n. or v.)

Don't use this verb in formal writing. Try [download](#), [exfiltrate](#), [extract](#), [gather](#), [remove](#), [retrieve](#), [take](#), or [view](#) instead.

### **dump files** (n.)

Files from memory dumps, core dumps, stack dumps, hex dumps, heap dumps, etc.

### **dust management**

### **DVD, DVR**

### **Dvorak**

An alternate keyboard setup that is efficient but uncommon. Pronounced "duh-vor-ack."

Don't confuse it with the classical composer Antonin Dvořák.

Related: **QWERTY**

## **E**

### **eBay**

### **e-commerce** (n.)

### **EFF**

Electronic Frontier Foundation. A nonprofit digital rights advocacy group. [eff.org](http://eff.org)

Related: **net neutrality**

### **e.g.**

Means "for example" in Latin. Always followed by a comma. **i.e.** means "in other words." Choose wisely.

### **egress filtering, egress testing**

### **EICAR test file**

An antivirus test file that is intended to be found as a virus (though it's not actually malicious). Pronounced "eye-car."

### **Elasticfox**

A pen testing tool.

### **electric, electrical** (adj.)

### **electronic** (adj.), **electronics** (n.)

### **element**

If it's a type of element, use normal font. If it's a named element, use tech font as in "a `customErrors` element."

## **elevation of privileges**

A common strategy for attackers: start as a low-privilege user and find flaws in permissions to gain admin credentials. Also called “escalation of privileges.”

## **ELF, ELF<sub>s</sub>**

Executable and linkable format.

## **email**

Related: **BCC, CC, daemon, DKIM, DMARC, Gmail, inbox, listserv, mailbomb, outbox, phishing, spam, spoof, SpoofCheck**

## **email addresses**

Use tech font as in `style@bishopfox.com`.

## **email spoofing**

## **embedded devices**

Related: **IoT**

## **emoji, emojis**

We prefer to pluralize as “emojis,” but “emoji” can be the plural, too.

Related: **Animoji, IM, tikzpeople, Unicode Consortium**

## **-enabled (adj.)**

Always hyphenate.

Ex: [Wi-Fi-enabled](#)

## **-encoded (adj.)**

Always hyphenate.

Ex: [URL-encoded](#)

## **-encrypted (adj.)**

Always hyphenate.

Ex: [SSL-encrypted](#)

## **encryption (n.)**

## **end-of-life (adj.) (EOL)**

## **endpoint**

## **end-to-end secure boot chains**

## **end user (n.), end-user (adj.)**

## **Engadget**

## **enterprise security (ES)**

Related: **asset, IR plan, risk, security controls, severity, threat modeling**

## **entity encoding**

## **enumerate (v.), enumeration (n.)**

## **environment**

The scope of an engagement that is more than a single application, site, or network.

## **EOL**

End-of-life product lines are no longer supported. Spell out on first use.

## **ePHI**

Electronic personal health information.

Pronounced as letters.

Related: **PHI**

## **EPT**

External penetration testing. Spell out on first use in formal writing.

Related: **APT, IPT**

## **ePub**

## **error message**

Use normal font with quotation marks around system messages as in “The username or password is incorrect.”

## **escape (v.)**

Certain characters are used to specify formatting or code. “Escaping” those characters means that they are interpreted literally and not used for their special function.

Related: **metacharacter**

## **-established (adj.)**

Always hyphenate.

Ex: [well-established](#)

## **EternalBlue**

The MS17-010 vulnerability.

Related: **NSA**

## **Ethernet**

Capitalized because it’s a trademark.

## **EULA**

End-user license agreement. Spell out on first use. Pronounced “you-la.”

## **Everyone**

Fictional Anonymous-style hacker collective from the TV show Elementary.

## **exabytes (EB)**

Related: **units of measurement**

## **Excel columns**

Use normal font for the title of columns as in A2 and B15.

## **Excel formulas**

Use tech font for the content of Excel cells as in =HYPERLINK and =1+1.

## **except, exception**

### **excerpt (n.)**

A bit of quoted code.

### **executable (n. or adj.)**

As in “malware-infected executable.”

### **execute (v.)**

### **exercise (v.)**

To interact with as in “exercise an API.”

## **exfiltrate (v.), exfiltrated, exfiltrating**

### **explicit (adj.)**

### **exploit (v. or n.)**

## **exploit chain**

## **exploit video**

### **exposed (adj.)**

Describes applications or functions that are available to the public internet (not only to a private or internal network) and are therefore vulnerable to attack.

### **eye-tracking (adj.)**

## **EyeWitness**

A pen testing tool.

# F

## Facebook

### facepalm

Related: **headdesk**

### FaceTime

An Apple videoconferencing product.

### -facing (adj.)

Always hyphenate.

Ex: [client-facing](#), [internet-facing](#)

### FairPlay

Apple DRM technology.

### false flag

A piece of evidence (e.g., an old digital certificate) planted by hackers to deliberately mislead investigators about their identity.

### false positives (n.)

### FAQ

Frequently asked questions. Pronounced as letters or “fack.” Write “an FAQ” in reports.

Related: **a vs. an**

### fat-finger (v.), fat-fingered (adj.)

To make a typo on a mobile device by pressing a nearby button.

### FBI

The Federal Bureau of Investigations.

Related: **CIA, Interpol, DHS**

### FCC

The Federal Communications Commission.

### FDA

The Federal Drug Administration.

### FDE

Full disk encryption. It’s the same as whole disk encryption. Spell out on first use.

### FERPA

The Family Educational Rights and Privacy Act of 1974 protects the privacy of student education records. Spell out in first use.

Related: **PII**

### fetch (v.)

### FFEIC

The Federal Financial Institutions Examination Council. Spell out in first use.

### FFmpeg

### field

If writing about a type of field, use normal font. If it’s a named field, use tech font as in “address field.”

### the Fifth Amendment

Among other things, it protects US individuals from self-incrimination.

Related: **EFF, encryption, Security Without Borders**

### file extensions

Capitalize the filename type if writing about the type, lowercase in tech font with a dot if writing the exact name, e.g., “the XML file” or “the PoC.xml file” or “PoC.xml.”

**filename** (n.)

**file path** (n.)

Use tech font to show file paths as in  
C:\Users\Fox\Downloads\fox.gif.

**file shares** (n.)

**file size** (n.)

**filesystem** (n.)

**file type** (n.)

**filter** (v. or n.)

**FinFisher, FinSpy**

Related: **spyware**

**fingerprint, fingerprinted** (v.)

**fingerprints**

Unique public key identifiers. Use tech font as in SubjectPublicKeyInfo fingerprints.

**FIPS tests**

Federal information processing standard.

**Fire TV**

An Amazon media player.

**firewall**

**FireWire**

**Fitbit**

**fixed-width** (adj.)

**flags**

Use tech font as in “the HttpOnly flag.”

**flame war** (n.)

**Flash, Flash Player**

An Adobe media player.

**flat files**

**flatscreen** (adj. or n.)

**flow chart** (n.)

**FOIA**

The Freedom of Information Act.

**follow up** (v.), **follow-up** (n. or adj.)

**footprinting** (n.)

**force-browse** (v.)

**forceful browsing** (n.)

**forensic watermark**

**forge, forging** (v.)

**formula, formulas**

**foxes**

Bishop Fox employees.

**FPS**

First-person shooter video game.

**fps**

Frames per second. Put a space between the number and the unit as in “60 fps.”

Related: **units of measurement**

**FQDN**

Fully qualified domain name. Spell out on first use.

**frameable** (adj.)

Related: **clickjacking**

**frame busting** (n.)**frame rate** (n.)**framework**

Write frameworks in normal font as in Crowbar and MVC-based framework.

**free-form** (adj.)**Free Software Foundation (FSF)**

A nonprofit organization.

Related: **EFF**, **open source**

**front door** (n. or adj.)

Related: **backdoor**

**front end** (n.), **front-end** (adj.)**fsociety**

A fictional Anonymous-type organization from the USA TV show Mr. Robot.

**FTC**

The Federal Trade Commission.

**FTL**

"Faster than light" warp drives in the TV show Battlestar Galactica and other sci-fi.

**FTP**

File Transfer Protocol.

**FUD**

Fear, uncertainty, and doubt. Pronounced "fudd."

**fullz** (n.)

A package of PII that can be bought on the black market. It usually includes SSN, DOB, and full name.

**function** (n.)

Capitalize the name of a function as in "the Forgot Password function."

**functionality**

Business jargon. Better to describe specific functions or features.

**function key**

Use normal font as in F1 and F8.

**fuzzer, fuzzing**

A fuzzer generates or mutates input for consumption by the target program with the intention of finding bugs.

**fuzz testing harness**

A framework that handles the crashes that result from a fuzzer.

**FXL**

Feature extraction language.

# G

**Game Boy****GameCube**

## game jam

A video game hackathon.

## Game of Life

A programmable simulation created by mathematician John Conway that featured patterns including pulsars and gliders.

## Gamergate

### -gapped (adj.)

Always hyphenate.

Ex: [air-gapped](#)

## gateway (n.)

## GaymerX

LGBTQIA-focused gaming conventions in California, New York, and Australia.

## GB

Gigabytes. No space between the number and unit as in "75GB." Do not pluralize GB.

## GBps vs. Gbps

Capitalization matters. GBps is gigabytes per second. Gbps is gigabits per second.  
Related: **units of measurement**

## GC

Short for garbage collection. Automatic memory management. Spell out on first use.

## Gchat

Google chat system.

## geocache, geocaching

## geolocation

## getID3()

A PHP media file parser.

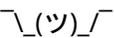
## GET request

## GHz

Gigahertz. Put a space between the number and the unit as in "2.4 GHz."

Related: **units of measurement**

## GIF file, .gif file

Pronounced "giff" or "jiff." 

Related: **file extensions**

## GIGO

Garbage in, garbage out. Say the whole phrase out loud or "gee-go."

## Girls Who Code

A nonprofit organization that runs clubs and programs to train girls to code.

<https://girlswhocode.com/>

## GitHub

A code repository. Our account is

<https://github.com/bishopfox>.

## GitLab

## Git repository, .git repository

A Linux version control system.

## GLBA compliance

The Gramm-Leach-Bliley Act of 1999 is a standard of security for financial institutions.

Related: **PCI compliance**

## globbing

Filename expansion through wildcards.

## **Gmail, example@gmail.com**

Related: **email address**

## **GNU**

Short for "GNU's Not Unix!" An operating system. GNU is a recursive acronym.

Pronounced "guh-new."

## **Go**

A programming language.

Related: **Golang**

## **Godwin's Law**

This law of the internet states that all arguments eventually devolve into someone comparing someone to Hitler.

Related: **Rule 34, message board, troll**

## **Golang**

This term is used when researching the programming language Go, which is a difficult keyword to search on its own.

## **golden master**

Related: **beta**

## **gold image**

Another term for base image or configuration baseline.

## **goodput**

Related: **badput, throughput**

## **Google**

Related: **Android, Chrome, Gchat, Gmail**

## **google (v.)**

## **Google Assistant**

Google Home AI.

Related: **Alexa, Cortana, Siri**

## **Google Drive**

## **Google Search**

The query engine that googles things. It responds with Google Search results.

## **GoPro**

## **GPG**

Gnu Privacy Guard. Also written as GnuPG. Spell out on first use.

## **GPO**

Group Policy Object. Spell out on first use.

## **GPS**

Global positioning system. Spell out on first use.

## **GPU**

Graphics processing unit.

## **Gradle**

An open source build tool.

## **grandfather clause**

## **gray-box testing**

Related: **black box, white box**

## **gray goo or grey goo**

An end-of-the-world scenario caused by the proliferation of self-replicating robots who eat the environment so all that is left is grey goo. Also refers to mushy bits of poorly written code. Do not use in formal writing.

Related: **kluge**

## gray hat

Related: **black hat**, **white hat**

## grayed out (adj.)

## grep (n. or v.)

“Get regular expression.” Can refer to the GNU tool of the same name or to mean “search” as in “I grepped for secret and found a password in source code.”

Related: **regex**

## greylisting

Even though American English uses gray-box and gray hat, greylisting is written with an “-ey” regardless of location.

## grok (v.)

To fully understand, to get.

## Grumpy Cat

I had a definition once. It was terrible.

Related: **lolcat**, **meme**

## Guccifer, Guccifer 2.0

Hackers who claimed to be behind the 2016 DNC hacks. Pronounced as “goo-chee-fer” or “goo-see-fer.”

## GUI

Graphical user interface. Pronounced “gooey.”

## GUID

Globally unique identifier. Pronounced “goo-widd.” Spell out on first use.

## GWT

Google Web Toolkit. Spell out on first use.

# H

## H-1B visa

A U.S. work visa for specialty occupations.

## H.264 (n.), H.264-encoded (adj.)

## hack (n. or v.)

Do not use in formal writing. Try [exploit](#), [gain access](#), [steal](#), or a more specific verb that applies to the situation.

Related: **cyber-**

## hackathon

## hacker

Do not use in formal writing. Use [attacker](#), [external threat](#), [malicious user](#), [consultant](#), [security researcher](#), [data scientist](#), or their job title, depending on the context.

Related: **Halt and Catch Fire**, **Mr. Robot**, **Silicon Valley**, **Sneakers**, **WarGames**

## Hacker Dojo

A Bay Area tech community.

## HackerOne

A vulnerability coordination and bug bounty platform.

## Hackers

1995 movie about hacking the Gibson and the planet.

## hactivist

## Hadoop

An Apache framework.

## **HAL 9000**

A fictional AI from 2001: A Space Odyssey.

## **Halt and Catch Fire**

AMC TV show about hacking, set in the 1980s.

## **hamburger button**

An icon with three horizontal lines that shows hidden menu options when clicked.

## **ham radio**

## **handheld** (adj.)

## **handle** (n.)

Related: **avatar, IRC, username**

## **hang** (v.)

When a server or computer hangs, it is non-responsive. If the requesting computer gives up waiting for a response, it times out.

## **haptic feedback**

## **hardcode** (v.), **hard-coded** (adj.)

## **hard copy** (n.), **hard-copy** (adj.)

## **hard drive** (n.)

## **harden** (v.)

To configure applications, systems, or services in a more secure manner, often using common guidelines.

Related: **best practices**

## **-hardening** (n. or adj.)

Always hyphenate.

Ex: [host-hardening](#), [system-hardening](#)

## **hardware**

## **hashcat**

A pen testing tool.

## **hashed** (adj.)

Related: **password, salt**

## **hash functions**

## **hashtag** or **#**

Only pronounce as hashtag when categorizing, not just any use of the [#] character, e.g., #octothorpe #poundsign

Related: **C#**

## **HAZOP**

A hazard and operability study.

## **HDTV**

Related: **flatscreen, on-demand, ratio**

## **headdesk** or **/headdesk** or **\*headdesk\***

An act of frustration and defeat.

Related: **facepalm**

## **header**

If it's a type of header, use normal font. If it's a named header, use tech font as in "an Origin header."

## **headless browser**

## **HEAD request**

Related: **GET request**

## **heap-based buffer overflow**

## **Heartbleed**

An OpenSSL bug.

**hex** (n.), **hex-encoded** (adj.)

## **HID**

Short for human interface device. The USB Rubber Ducky is a keyboard HID. Spell out on first use.

**highest-severity** (adj.)

**high-impact** (adj.)

**high-performance** (adj.)

**high-speed** (adj.)

**high-value** (adj.)

**hijack, hijacking** (n. or v.)

An umbrella term for attacks that take over controls or assume the role of a user and compromise the system. Avoid the verb when possible in formal reports. Try [take over](#) or [take advantage of](#) instead.

Related: **browser hijacking, juice jacking, page-hijacking**

## **HIPAA**

The Health Insurance Portability and Accountability Act. Pronounced “hippa.”

Related: **ePHI, PHI**

## **HLS**

HTTP Live Streaming. Spell out on first use.

## **HMAC**

Hash-based message authentication code. Pronounced “H-mack.” Spell out on first use.

**homepage** (n.)

## **HomePod**

Apple smart speaker.

Related: **Internet of Things**

**homescreen** (n.)

**honey accounts**

Related: **canary account**

**honeybot**

A Twitterbot troll.

**honeypot**

**honeytokens**

**hook** (v.), **hooked** (adj.), **hooking** (n.)

## **Hopper**

A pen testing tool.

## **host**

Use tech font as in 10.0.7.180.

Related: **localhost, URI**

**-hosted** (adj.)

Always hyphenate.

Ex: [self-hosted](#)

**host-hardening** (adj.)

Related: **harden**

**hostname** (n.)

**hotfix, hotfixes** (n.)

**hotlink, hotlinking** (n.)

**hotspot** (n.)

**hot-swap** (v.)

## hot wallet

Online bitcoin storage.

Related: **cold wallet**

## hotwire (v.)

## hover (v.)

## how-to (n. or adj.) how to (v.)

We published a [how-to](#). This is [how to](#) do it.

## Hping

A security tool. Pronounced “H-ping.”

## HPP

HTTP Parameter Pollution. Spell out on first use.

## HSTS

HTTP Strict Transport Security. Spell out on first use.

## h/t

Informal. Short for hat tip. A way of thanking someone online for being or providing a source.

## HTML, HTML5

Hypertext Markup Language. Do not spell out.

## http://, https://

No need to include these in URIs unless the presence or lack of secure HTTP is relevant to the narrative.

## HTTP statuses

Capitalize HTTP statuses in normal font as if they were titles. Use quotation marks if they might be confused with nearby text.

Ex: [200 OK](#), [404 Page Not Found](#), [HTTP 413 Request Entity Too Large](#), [500 Internal Server Error](#)

Related: **error message**, **titles of published works**

## HttpOnly integrate

## HTTPOxy

## HTTP response splitting

## HTTP.sys

A kernel mode driver.

## humblebrag

A disingenuous public complaint that slyly boasts about an enviable life.

## hyperspace (n.)

## hypertext (n.)

The “HT” in HTML and HTTP.

## hyperthreading (HT)

Spell out on first use.



## I2P

Short for Invisible Internet Project. An anonymous communication network. Do not spell out.

**i18n**

Internationalization. 18 represents the 18 letters removed from the middle of the word.

Related: **a11y, l10n, k8s**

**IaaS**

Infrastructure as a service. If spoken, say the whole phrase, not the acronym. Spell out on first use.

Related: **KMaas, PaaS, SaaS**

**IAM**

AWS Identity and Access Management. Spell out on first use.

**IANAL**

Informal. "I am not a lawyer."

**ICMP**

Internet Control Message Protocol. Spell out on first use.

**IDE, IDEs**

Integrated development environment. Spell out on first use.

Related: **line numbers, source code**

**IDOR**

Insecure direct object references. Spell out on first use.

**iDRAC**

Integrated Dell Remote Access Control.  
Related: **DRAC**

**IDS**

Intrusion detection system. Spell out on first use.

**i.e.**

Means "that is to say" in Latin. Always followed by a comma. **e.g.** means "for example." Choose wisely.

**iframe or i frame tag**

Short for inline frame. IFrame and iFrame also appear in texts, but we lowercase.

**IFTTT**

Short for If This Then That. A service where users can create conditional statement chains called recipes. Pronounced as "ift."

**IIRC**

If I recall correctly.

**IIS, IIS Express**

Microsoft Internet Information Services software.

**IKE, IKEv1, IKE v2**

Internet Key Exchange.

**iLO**

HP Integrated Lights Out.

**ILSpy**

A pen testing tool.

**IM (n. or v.)**

Instant message. Spell out in formal writing.  
Related: **Gchat, IRC, Signal, WhatsApp**

**Imgur**

A photo-hosting website company with a giraffe mascot. Pronounced "imager."

**implementable (adj.)****implicit (adj.)**

## **improper MIME type**

## **improperly scoped cookies**

## **in-band** (adj.)

As in “in-band reflection of file contents.”

Related: **out-of-band**

## **inbound** (adj.)

## **inbox** (n.)

## **incident response (IR) plan**

Use lowercase when writing about the concept of the plan. Capitalize it if referring to the name of a specific document.

Related: **IR plan**, **SIR plan**

## **infiltrate** (v.)

## **infosec**

Informal. Intelligence communities use this term to describe the information security industry.

## **information security**

This industry is also called infosec, cybersecurity, and internet security.

## **information superhighway**

Don't use this to describe the internet.

## **in-game** (adj.)

## **in-house** (adj.)

## **init script**

Boot script for Unix.

## **injection** (n.)

## **inline** (adj.)

Code that is in line with other code. The CSP rule is called `unsafe-inline`.

## **input** (v. or n.)

## **in-scope** (adj.)

## **insecure vs. not secure**

These are sometimes used interchangeably and sometimes they mean very different things. Define briefly on first use to clarify your intended meaning.

## **insecure cookie transmission**

## **insourcing**

The opposite of outsourcing.

## **Instagram**

## **instance count**

The number of unique locations in a codebase, system, or network that require modification to remediate a finding.

## **interface** (n. or v.)

As in “exposed administrative interface.”

## **internet** (n.)

## **The Internet Archive**

A nonprofit library and archive of historical web pages. <https://archive.org/>

Related: **net neutrality**

## **Internet Explorer (IE)**

The Internet Explorer web browser.

## Internet of Things (IoT)

Consumer-grade embedded devices.  
Related: **app** vs. **application**, **Fitbit**,  
**motion-activated**, **smart-**, **Wi-Fi**

## Interpol

The international police organization.

## invalidated vs. unvalidated

**Invalidated** data has been checked and deemed invalid. **Unvalidated** data has not been checked at all.

## iOS

Apple mobile platform. Because of the lowercase “i,” avoid beginning sentences with this term if possible.

## IoT

Internet of Things.

## IP

Short for Internet Protocol or intellectual property, depending on context. For clarity, spell out “intellectual property” on first use in technical writing.  
Related: **IP address**

## iPad, iPod

### IP address

Short for Internet Protocol address.  
Use tech font as in 10.40.131.22.  
Related: **port numbers**, **URL**

## iPhone 5s, iPhone 6 Plus, iPhone X

Apple smartphones.

## IPMI

Intelligent platform management interfaces. Spell out on first use.

## IPP

Internet Printing Protocol.

## IPS

Intrusion prevention system. Spell out on first use.

## IPsec

Internet Protocol Security. Spell out on first use.  
Related: **infosec**, **OPSEC**, **PERSEC**

## IPT

Internal penetration testing. Spell out on first use.  
Related: **APT**, **EPT**

## IR plan

Short for Incident Response plan. Spell out on first use.

## IRC

A messaging system. Internet Relay Chat.  
Related: **handle**, **UGT**

## IRL

In real life.

## ISAC

Information Sharing and Analysis Center. Pronounced “eye-sack.” Spell out on first use.

## **ISO/IEC 27001**

A common information security framework that determines international standards for many types of technology and equipment. ISO is pronounced “eye-so.”

## **ISP**

Internet service provider. Spell out on first use in public-facing documents.

## **IT Crowd**

A British sitcom about a tech support department.

# **J**

## **jack**

As in “Ethernet jack.” Better to use “port” in formal writing.

## **jailbreak (v.)**

To modify a mobile device (e.g., a smartphone) past the limits set by the manufacturer to gain privileged access.

Related: **sandbox escape**

## **jailbroken (adj.)**

Describes a user-modified mobile device.

## **Java EE**

Java Enterprise Edition. Do not abbreviate as JEE.

## **JavaScript (JS)**

A programming language.

## **JBoss**

Java middleware.

## **JCE**

Java Cryptography Extension.

## **Jenkins**

## **JIRA**

Workflow and issue tracking product. Not an acronym. Pronounced “jeera.”

## **JMX**

Java Management Extensions. Spell out on first use.

## **JPEG file, .jpeg file**

Pronounced “jay-peg.”

Related: **file extensions**

## **jQuery**

## **JSON, JSONP**

Short for JavaScript Object Notation. JSONP is short for “JSON with padding.”

Pronounced as J-sahn and J-sahn-P.

## **JSP file, .jsp file**

Related: **file extensions**

## **juice jacking (n.)**

## **Julia**

A programming language.

## **jumpbox**

Better to use “proxy” or “attacker’s server” in formal writing. Also called a jump host or jump server.

## jump drive

Informal. Use USB drive, flash drive, or thumb drive instead, depending on the context.

Related: **USB drive**

## junk mail

Related: **spam**

## JVM

Java virtual machine. Spell out on first use.

# K

## k8s

Kubernetes. 8 represents the 8 letters removed from the middle of the word.

## Kali Linux

## Kaspersky Labs

An international security firm headquartered in Russia.

## KB

Kilobytes. No space between the number and unit as in "50KB." Do not pluralize KB.

Related: **units of measurement**

## keepalive, keepalives (KA) (n.)

Keepalive packets.

## KeePass

Password management software.

## kernel, kernel panic

## keyboard keys

Capitalize keys like Enter and Caps Lock. Use hyphens to show combinations like Control-Alt-Delete or Option-N.

Related: **Dvorak, function key, punctuation, QWERTY, wildcards**

## keygen, keygens

Key generators.

## keylogger, keylogging

## key pair (n.)

## keyspace (n.)

## keystroke (n.)

## Keywhiz

Password management software.

## keyword (n.)

## kHz

Kilohertz as in "535 kHz." Do not pluralize kHz.

Related: **units of measurement**

## Kickstarter

Related: **crowdfund**

## kill chain (KC) (n.)

## kill switch (n.)

## kluge or kludge

Bad code.

## **KMaas**

Key management as a service. If spoken, say the whole phrase, not the acronym. Spell out on first use.

Related: **IaaS, PaaS, SaaS**

## **KMS**

Key management service. Spell out on first use.

## **knowledge base**

## **KRACK**

A Wi-Fi-based vulnerability.

## **Kubernetes or k8s**

Pronounced "coober-nettees."

Related: **Docker**

# **L**

## **L10n**

Localization. 10 represents the 10 letters removed from the middle of the word.

Related: **a11y, i18n, k8s**

## **LAN**

Local area network.

## **LanMan hash**

Short for LAN Manager hash. We prefer to write it out or abbreviate to LM hash.

## **LAN Turtle**

A pen testing tool for getting shells.

## **LARP, larping** (n. or v.)

A live action role-playing game.

## **LastPass**

Password management software.

## **LaTeX**

A document preparation system.

Pronounced "lay teck."

Related: **tikzpeople**

## **Layer 3 firewall rules**

## **LCD, LCDs**

Liquid crystal display monitors. Do not spell out.

## **LDAP**

Lightweight Directory Access Protocol.

Pronounced "el dap." Spell out on first use.

## **LDAP Admin**

A pen testing tool.

## **leak, leaked, leaking**

## **LED, LEDs**

Light-emitting diode. Do not spell out.

## **Leet or 1337 or Leetspeak or l33tsp34k**

A coded form of online writing featuring codified typos and a combination of numbers and punctuation.

Ex: [H4X0R](#), [n00b](#), [pr0n](#), [pwn](#), [teh](#)

## **-level**

Always hyphenate in adjectives.

Ex: [lower-level](#)

## **leverage** (v.), **leveraged** (adj.)

## **LFI**

A local file inclusion vulnerability. Spell out on first use.

## **LGBTQIA**

Lesbian, gay, bisexual, transgender, queer, intersex, asexual. For more guidance on inclusive language, please consult <http://consciousstyleguide.com/>.

## **lifecycle management**

Related: **SDLC**

## **life hack** (n.)

## **Lightning cables** (n.)

## **Like** (v. or n.)

Facebook verb of approval.

## **likelihood** (n.)

## **limit** (v.)

To control the scope, impact, or types of attacks. Also try [filter](#), [narrow](#), or [omit](#).

## **linefeed characters**

## **line numbers**

Use normal font as in "line 1337 of the code." Don't use commas in line numbers.

## **LinkedIn**

## **Linux**

An open source OS. Thanks, Linus Torvald!  
Related: **Debian**, **init script**, **RedHat**, **Unix**

## **listserv**

The company is called LISTSERV. The generic term is "listserv" or "email list."

## **little-endian** (adj.)

## **livestream** (v.), **livestreaming** (n.)

## **live-tweet** (v.)

## **LLMNR**

A modern Windows protocol. Link-Local Multicast Name Resolution.

## **LM hash**

LAN manager hash.

Related: **NTLM hash**

## **LMS**

Learning management system. Spell out on first use.

Related: **CAM**

## **load-balance** (v.), **load balancing** (n.)

## **localhost**

A hostname that always refers to the computer you're using. The localhost IP address is 127.0.0.1.

## **localStorage**

## **lockout policy**

## **lock picking**

The skill of picking locks.

Related: **smart lock**

## **lock screen** (n.)

## **log files**

## **logged-in** (adj.)

As in "a logged-in user."

## **log in** (v.), **login** (n.)

## **login page**

**log out (v.), logout (n.)**

## **LOIC**

Low Orbit Ion Cannon. An old-school way to crowdsource a DoS attack. Pronounced “low-ick.”

## **lolcat**

I can has internet language?

Related: **doge, Grumpy Cat, meme**

## **lookahead parameter**

## **look up (v.), lookup (n.)**

## **lossy compression**

## **lowercase (adj.)**

## **LSASS**

Local Security Authority Subsystem Service.

## **LTE**

Long Term Evolution. A high-speed wireless communication standard.

Related: **3G, 4G**

## **LTS**

Short for long-term support. Versions of software that are intended to last longer than normal. Spell out on first use.

## **Lucius Fox**

A character from the Batman canon, played by Morgan Freeman in Christopher Nolan’s trilogy. Lucius Fox is an inventor and runs WayneCorp. Because of his defensive hacking skills, we use his name in our company name.

Related: **Martin Bishop**

## **Lucky Thirteen attack**

# **M**

## **M.2**

An expansion port and SSD.

## **MAC**

Message authentication code. Spell out on first use.

Related: **HMAC**

## **MAC address**

Short for media access control address. A unique identifier on a network-enabled device. One level below IP address.

## **MacBook**

## **machine learning (ML)**

## **macOS-based (adj.)**

## **MAC OS X**

## **macro (n.)**

OK in formal writing if relevant, but use “automation” for the general technique.

## **mailbomb**

Related: **email, dox, phishing, spam**

## **MailChimp**

## **mainframe (n.)**

## Maker Faire

A global series of DIY community events that started in the Bay Area.

<http://makerfaire.com/>

Related: **Arduino, how-to, life hack, Raspberry Pi, servo**

## Malbolge

An esoteric programming language.

## malformed (adj.)

A syntactically improper bit of data or code.

## malicious actor

This represents a wide range of potential attackers from individuals to nation-states. When writing about individual threats, use [attacker](#) or [malicious user](#).

## malicious code

## malware

Malicious software. A catch-all term for anything that could be called malicious including CryptoLockers, spyware, viruses, trojans, and backdoors.

## malware-infected executable

## Man-in-the-Browser attack (MitB)

When spoken, pronounce the phrase, not the acronym.

## Man in the Middle (n.),

## Man-in-the-Middle (adj.) (MitM)

Short for Man-in-the-Middle. When written as MitM, precede with “an.” If spoken, say the whole phrase, not the acronym.

Related: **a vs. an**

## mapping (n.)

## MariaDB

An open-source clone of MySQL.

## markdown (n.)

## marketplace (n.)

## markup (n.)

## markup language

HTML and XML are markup languages.

## Martin Bishop

A character played by Robert Redford who leads a security consulting team in the 1992 movie Sneakers. Because of his offensive hacking skills, we use his name in our company name.

Related: **Lucius Fox**

## mass assignment

## MB

Megabyte. No space between the number and unit as in “75MB.” Do not pluralize MB.

Related: **MiB, units of measurement**

## Mbps

Megabits per second. No space between the number and unit as in “500Mbps.”

Related: **units of measurement**

## mechanism

Put the name in tech font as in “`protect_from_forgery` mechanism.”

## media

Related: **Blu-ray, CD, GoPro, MP3**

## Meltdown

A flaw that affects Intel, AMD, and ARM chipsets. It was publicly disclosed in January 2018.

Related: **Spectre**

## Memcache, Memcached

A memory caching server.

## meme

Pronounced “meem.”

Related: **4chan, doge, Grumpy Cat, lolcat, milkshake duck, rickrolling**

## message board

Related: **ATM, handle, headdesk, IANAL, IIRC, NSFL, NSFW, tl;dr, PEBKAC, RTFM**

## metacharacter

A character with a special meaning in a programming language or regex. It must be set apart (escaped) with another character to use its literal meaning, as in “**\***” vs. **\***.

Related: **\n**

## metadata

## Metasploit

A pen testing tool.

## Meterpreter

A pen testing tool.

## MFA

Multi-factor authentication. Spell out on first use in public-facing docs to avoid confusion with a Master of Fine Arts degree.

Related: **2FA**

## MHz

Megahertz as in “100 MHz.”

Related: **units of measurement**

## MiB

In Base 2, 1 mebibyte (MiB) is 1,024 kibibytes (KiB). 1 kibibyte is 1,024 bytes. Megabytes (MB) are in Base 10.

Related: **bytes, MB**

## microblogging (n.)

## microservice (n.)

## Microsoft

Related: **Cortana, MS SQL, Windows**

## MIDI

Musical instrument digital interface. Do not spell out. Pronounced “mid-ee.”

## military-grade encryption

May refer to AES-256 encryption. Do not use this term; refer to the type of encryption by name instead.

## milkshake duck

A hypothetical wholesome new public figure who is quickly revealed to be vile.

Related: **Godwin’s Law, meme**

## millennial

Marketing jargon. When broadly used, this includes people born between 1980 and 2010. It’s better to use other demographic markers (such as age ranges).

## MIME

Multipurpose internet mail extensions. Do not spell out. Pronounced “mime.”

**Mimikatz**

A pen testing tool.

**mirroring** (n.)**mirror site** (n.)**mission-critical** (adj.)**mitigate** (v.)

To lessen the impact of potential future attacks. Not interchangeable with “reduce.”

**mitigation** (n.)

The application of compensating controls to decrease the impact of identified vulnerabilities while not fully remediating those vulnerabilities.

**MitM**

Short for Man-in-the-Middle. When written as MitM, precede with “an.” If spoken, say the whole phrase, not the acronym. In cryptography, this can also refer to the Meet-in-the-Middle attack.

Related: **a** vs. **an**

**mm/dd/yyyy**

When recommending limitations on allowable characters in date fields, write the month/day/year format in tech font.

Related: **date**, **year**

**mobile devices**

Smartphones and tablets.

**mod** (v. or n.)

Informal. To modify.

**model number**

Use normal font for software version numbers, product model numbers, serial numbers, and builds.

**Moore’s Law**

About every 18 months since 1965, the number of transistors per square inch on integrated circuits has doubled. Observed by Intel co-founder Gordon Moore.

**MOTD**

Message of the day banner.

**motherboard jumpers****motion-activated** (adj.)**motion capture, mo-cap** (n. or adj.)**mouseover** (adj. or n.), **mouse over** (v.)**mousepad****Mozilla Firefox****MP3, .mp3 file, MP4, .mp4 file**

Music files.

Related: **file extensions**, **MIDI**

**Mr. Robot**

TV show about a paranoid hacker that sometimes uses Bishop Fox exploits.

Related: **fsociety**, **Kali Linux**, **Raspberry Pi**, **Tastic RFID Thief**

**ms**

Milliseconds. Put a space between the number and the unit as in “250 ms.”

Related: **units of measurement**

## MSA

Master service agreement. Spell out on first use.

Related: **SOW**

## MSDE

Microsoft SQL Server Data Engine. Spell out on first use.

## MSFvenom

A pen testing tool.

## MSI file, .msi file

A Windows installer package file format.

## MS SQL

Microsoft SQL server.

## multi-factor authentication (MFA)

Spell out on first use in public-facing docs to avoid confusion with a Master of Fine Arts degree.

Related: **2FA**

## MVC

Short for the Model-View-Controller architectural pattern. Spell out on first use.

Related: **ASP.NET**

## MySQL

# N

## \n

The newline character is an invisible special character that moves the text to the next vertical line down.

Related: **carriage return character**

## NAC

Network access control. Pronounced “nack.” Spell out on first use.

## nameserver

An internet server that resolves domain name queries. Part of DNS.

## NAND gate

Short for negative-AND gate. A logic gate that produces a false output only if all of its inputs are true.

## nanotechnology (n.)

## nation state (n.)

## NBNS

A modern Windows protocol. NetBIOS Name Service.

## NDA

Non-disclosure agreement. Spell out on first use in public-facing documents.

## need to know (v.), need-to-know (adj.)

The user does not [need to know](#) this. Intel is given on a [need-to-know](#) basis.

## NetBIOS

Network basic input/output system.

## netblock

A range of IP addresses.

## Netcat or nc

A utility that reads from and writes to network connections with TCP or UDP.

## Netflix

## **.NET Framework**

A Microsoft software framework. If possible, don't begin sentences with this term.  
Pronounced "dot net."

## **Netgear or NETGEAR**

## **net neutrality**

Related: **EFF, FCC, Free Software Foundation, The Internet Archive, ISP**

## **net risk**

Overall risk.

## **network security**

Alternate term for information security.

## **network segmentation**

## **NFS**

Network File System.

## **NfSpy**

A pen testing tool.

## **Nginx**

Web server software. Pronounced "engine X."

## **ngrep**

Network grep. Pronounced "N-grep."  
Related: **tgrep**

## **Nintendo Switch**

## **NIST**

National Institute of Standards Technology.  
Pronounced "nist."

## **NIST CSF controls**

## **Nmap, Nmap scan**

Short for Network Mapper. A pen testing tool used to scan ports and map networks.

## **NOC**

Network operations center. Pronounced as "nock."

## **node**

## **Node.js**

An open source JavaScript runtime environment.

## **nonce, nonces (n. or adj.)**

## **non-disclosure agreement (NDA)**

## **nosni ff**

## **NotPetya**

## **NSA**

The U.S. National Security Agency.

## **NSFL**

Not safe for life/lunch.

## **NSFW**

Not safe for work.  
Related: **CW, TW**

## **NTLM hash**

NTLM protocol uses two hashed password values: the LM Hash and the NT Hash.

## **NTLMv2**

Short for NT LAN Manager. A suite of Windows security protocols.

## **null byte character, null byte injection**

## NULL session

### numbers

Per AP style, write out numbers below ten, except in set phrases. Write numbers plainly, without superscript. Plural years like “in the 1990s” do not take an apostrophe. Non-year numbers have a comma every 3 digits as in “525,600 minutes.”

Related: **date**, **IP address**, **model numbers**, **mm/dd/yy**, **phase**, **pixel**, **port**, **ratio**, **units of measurement**, **version numbers**, **year**

### NVD

National Vulnerability Database.  
<https://nvd.nist.gov/>

Related: **CVE**

# O

### OAuth

An authentication protocol. Pronounced “oh-auth.”

### obfuscation

Related: **security through obscurity**

### Objective-C

A programming language.

### oclHashcat

A pen testing tool.

### OCR

Optical character recognition. Spell out on first use.

Related: **PDF**

## Oculus Rift

### OData

OData is a RESTful means of exposing access to a data store.

### OEM

Original equipment manufacturer. Spell out on first use.

Related: **software piracy**

### offboarding (n.)

Opposite of onboarding.

### off-chain (adj.)

Off-the-block cryptocurrency transactions.

Related: **bitcoin**, **coins** vs. **tokens**

### offline (adj.)

### offscreen (adj.)

### off-site (adj.)

As in “off-site redirect.”

Related: **on-site**

### OGNL

Short for object-graph navigation language, an open source language. Vulnerable to injection attacks. Pronounced “ogg-null.”

### OK

Do not use in formal reports outside of quoted code and tables.

### ...omitted for brevity...

This phrase indicates that irrelevant parts of the quoted code have not been included.

Related: **[REDACTED]**

### on-air (adj.)

**onboarding** (n.)

**on-demand** (adj.), **on demand**

[On-demand](#) services. Services [on demand](#).

**one-time** (adj.)

**ongoing** (adj.)

**.onion sites**

Hidden services on Tor.

**online** (adj. or n.), **on line**

Wikipedia is an [online](#) encyclopedia.

A functioning system is [on line](#).

**onscreen** (adj.)

**on-site** (n. or adj.), **on site**

It was an [on-site](#). It was an [on-site](#) engagement. The team was [on site](#).

**OOB**

Out-of-band. Spell out on first use.

**OOP**

Object-oriented programming. Spell out on first use.

**open access** (n. or adj.)

**open source** (adj.)

Software with its source code made available to encourage modifications.

Related: **The Cathedral and the Bazaar**

**OpenVPN**

Open source VPN software.

**operating system (OS)**

**OpManager Decrypter**

A pen testing tool.

**OPSEC**

Operations security.

**opt in** (v.), **opt-in** (adj.)

**opt out** (v.), **opt-out** (adj.)

**OS**

Short for operating system. Spell it out as “operating systems” to pluralize instead of “OS’s” or “OSes.”

Related: **macOS, Linux, Windows**

**OSCP**

Offensive Security Certified Professional.

**OSINT**

Open Source Intelligence. Pronounced as “O-S-int.”

**OTA**

Over-the-air (programming). Spell out on first use.

Related: **livestreaming, on-air**

**outbound** (adj.)

**outbox** (n.)

**outbrief** (n.)

**outdated** (adj.)

**outgoing** (adj.)

**out-of-band** (adj.) **OOB**

Spell out on first use.

**out-of-date** (adj.)

**out-of-scope** (adj.), **out of scope**

It was an **out-of-scope** server. The service was **out of scope**.

**outsourcing**

**OWA**

Outlook Web Access.

**OWASP**

Every few years, the Open Web Application Security Project curates a list of the top 10 threats in information security. Pronounced "oh-wasp." <https://www.owasp.org/>

**OWASP Zed Attack Proxy**

A web vulnerability proxy and scanner.

**-owned** (adj.)

Always hyphenate.

Ex: **client-owned**

## P

**PaaS**

Platform as a service. If spoken, say the whole phrase or "pass." Spell out on first use.

Related: **IaaS, KaaS, SaaS**

**page**

If it's a specifically titled web page, capitalize as in "the Forgot Password page."

**page-hijacking attacks**

**page view**

**pain points**

Business jargon but OK if used sparingly.

**PAN truncation**

PAN is short for primary account number. Credit card number display that only shows the last 4 digits as in "\*\*\*\*\*1234."

**parameter**

If writing about a type of parameter, use normal font. If it's a named parameter, use tech font, as in "siteCode parameter."

**parameterized queries**

Also known as "prepared statements."

**parse** (v.), **parser** (n.)

**passphrase**

Related: **password**

**pass-the-hash attack**

**password-protected** (adj.)

**passwords**

Use tech font for password examples as in `letmein` and `123456`.

Related: **KeePass, Keywhiz, LastPass**

**Pastebin** (n. or v.)

Can refer to the company or the general act of publishing something anonymously (like credit card numbers) on the internet, not necessarily on the Pastebin website.

**patch** (n. or v.)

An update to existing software that adds functionality, fixes bugs, or both.

## **patch cycle**

## **PATCH request**

## **path traversal**

Also known as directory traversal.

## **PAX**

Short for Penny Arcade Expo. A series of gaming conventions.

## **payload**

## **PayPal**

A mobile payment service.

Related: **Square Cash, Venmo**

## **paywall (n.)**

Avoid using this as a verb in formal writing.

Try “blocked by paywall” or “requires a login” instead.

## **PBKDF2**

A password-based key derivation function. Generally used interchangeably with cryptographic hash functions, although there are technical distinctions.

## **PCB**

Printed circuit board. Spell out on first use.

## **PCI**

Payment Card Industry.

## **PCI compliance**

Related: **GBLA compliance**

## **PCI DSS**

Payment Card Industry Data Security Standard(s).

Related: **PAN truncation, PIN**

## **PCIe**

A serial expansion bus standard. Peripheral Component Interconnect Express.

## **PCRE**

Perl-compatible regular expressions. Spell out on first use.

## **PDB file, .pdb file**

Program database file.

## **PDF, .pdf file**

## **PDQ Deploy**

An admin tool.

## **PEBKAC**

Problem exists between keyboard and chair. Pronounced “peb-cack.”

## **peer-to-peer (adj.)**

## **penetration testing, pen testing, (n.)**

Security testing in which evaluators mimic real-world attacks to identify ways to circumvent the security features of an application, system, or network. Pen testers look for chains of vulnerabilities that can be used together to gain more privileged or overall access.

Related: **APT, bug bounty, red teaming**

## **percussive maintenance (n.)**

Fixing things by hitting them. Do not use in formal writing.

## **Perl**

Short for Practical Extraction and Report Language. A programming language. Do not spell out.

## permissions

If writing about a type, use normal font. If naming a specific permission, use tech font as in "SET\_ALARM permissions."

## PERSEC

Personal security. Used in military contexts.  
Related: **InfoSec, OPSEC**

## persistence (n.), persistent (adj.)

Persistent access means an attacker continues to access a system or application over a long period of time.  
Related: **session fixation, shell**

## Petya

A ransomware attack that hit June 2017.  
Related: **NotPetya**

## pfSense

An open source firewall.

## PGP

Pretty Good Privacy. An encryption program.

## phase, Phase 1

If writing about phases generically, lowercase. If dividing a project into sections, capitalize individual phases as in "Phase 2."

## PHI

Protected health information. Pronounced as letters. Spell out on first use.  
Related: **ePHI, PII**

## phishing

Also known as email phishing.  
Related: **credentials, mirror site, social engineering, spear-phishing**

## photoshop (v.), photoshopped (adj.)

## PHP complex syntax, PHP curly syntax

## PHP magic methods

Certain PHP methods including `_construct`, `_get`, and `_set`.

## phreaking

Related: **hacker, social engineering**

## pickle

A Python object serialization protocol.

## pickled, pickling

Python object hierarchy converted into a byte stream (and therefore serialized).  
Related: **unpickling**

## PID

Process identifier. Pronounced as letters or "pidd." Spell out on first use.

## PII

Short for personally identifiable information as in full name, DOB, home address, phone number, or email address. Pronounced as letters. Spell out on first use.  
Related: **DOB, fullz, PAN truncation, password, PIN, SSN, username**

## PIN

Personal identification number. "PIN number" is redundant.

## ping (v., n., or adj.)

To initiate contact and wait for a response. Sometimes specifically refers to using the ping utility.

## **The Pirate Bay (TPB)**

### **pivot point**

A foothold that an attacker can use to gain further access into a system.

### **Piwik**

An open source analytics program.

### **pixel (n.)**

When describing the size of an image, list width then height with an “x” between as in “100x100 pixel image.” Put a space between the number and unit. No commas.

Related: **numbers, units of measurement**

### **PKI**

Public key infrastructure. Spell out on first use.

### **plaintext or plain text**

Can refer to either unencrypted text (like cleartext), the input to a cryptographic system, or simple, unformatted text (not rich text). In our reports, it is not a synonym with cleartext. Define briefly on first use to clarify your intended meaning.

Related: **cleartext, CPA**

### **platform agnostic (adj.)**

In this context, agnostic means that the entity does not have a preference towards any particular platform.

### **playbook**

### **playlist**

### **PlayStation**

Related: **PS2**

### **PLD**

Payload. Spell out on first use.

### **PL/SQL**

A programming language used by Oracle.

### **plug in (v.)**

### **plugin (n.)**

When referring to a plugin by name, put the name in tech font as in “wpgform WordPress plugin.”

### **p.m.**

Put a space after the number as in “2 p.m. PST.” Include the time zone if referring to a testing window or specific event.

### **PO**

Short for purchase order. Business jargon. Spell out on first use.

### **PoC**

Could refer to a “proof of concept” or a “point of contact” within the client company. Spell out on first use for clarity. Related: **proof of concept, T-POC**

### **podcasts**

Capitalize podcast names and use normal font as in Security Weekly.

Related: **titles of published works**

### **POODLE attack**

Short for Padding Oracle on Downgraded Legacy Encryption. A Man-in-the-Middle attack.

## **POP**

Property-oriented programming. Spell out on first use.

## **pop up (v.), pop-up (adj. or n.)**

## **Pornhub**

Related: **RedTube, Rule 34**

## **port**

As in "USB port." Use this term in formal writing, but "jack" is fine elsewhere.

## **portal**

An entranceway, e.g., an employee login page.

## **port numbers**

Write them without commas in normal font ([port 3389](#)) unless it appears at the end of an IP address (54.243.128.77:3389).

Related: **numbers**

## **port scan (n.)**

## **post (v. or n.)**

## **post-apocalyptic (adj.)**

Related: **grey goo, sci-fi, Skynet**

## **post-exploitation (adj. or n.)**

## **POST request**

Related: **request**

## **PowerBook**

## **PowerPoint**

## **power user (n.)**

## **preflight (n.)**

In CORS, the browser sends an OPTIONS request before the actual request to check that the server's response headers allow the user-agent to send the request. The request is dropped if the server response does not allow the request.

## **preimage**

An algorithm input. Commonly refers to cryptographic preimage attacks.

## **prepared statements**

Same as parameterized queries.

## **preset (n., v., or adj.)**

## **pretexting (n.)**

Related: **social engineering**

## **Pretty Theft module**

A BeEF module.

## **principle of least privilege**

The concept that users should have only enough permissions as necessary for their role in a system, not more.

Related: **need-to-know**

## **print out (v.), printout (n.)**

## **prioritize (v.)**

To rank vulnerabilities by severity level in the environment.

## **privacy protection**

## **privesc or privilege escalation**

Related: **elevation of privileges**

## **PRNGs**

Pseudo-random number generators. Equivalent to RNGs. (Pseudo refers to the fact that computers cannot make true random numbers, it is not a judgment about their security or quality). Pronounced as letters. Spell out on first use in public-facing documents. Related: **CSPRNG**

## **ProcDump**

A pen testing tool.

## **Procmon**

Short for Process Monitor. A Windows monitoring tool.

## **prod**

Informal. The system in production, as opposed to dev (development).

## **program** (n. or v.)

## **programming language**

Related: **BASIC, Brainfuck, C # FXL, Golang, HTML, JavaScript, Julia, Malbolge, Objective-C, OGNL, Perl, PL/SQL, Python, Ruby, SAML, Scala, VBScript, XML, YAML**

## **proof of concept** (n.),

## **proof-of-concept** (adj.) (**POC**)

The team created a [proof of concept](#). It was a [proof-of-concept](#) payload.

## **protocol**

How computers talk to each other.

## **ProtonMail**

## **provision** (v.)

As in “to provision one cluster on each account.”

## **proxy, proxying** (n. or v.)

Moving data through an intermediate, usually so that it’s easier to modify before sending it through. Proxy can refer to the intermediate or the act of moving the data.

## **PS2, PS3, PS4**

## **PSK**

Pre-shared key. Spell out on first use.

## **PSR**

PHP Shared Recommendation. PSR-0 to PSR-3.

## **public address spaces**

## **public-facing** (adj.)

## **public key, public key encryption**

## **publicly known** (adj.)

## **PubNub**

## **punctuation**

Related: **characters, metacharacters**

## **purple team**

Related: **blue team, red team**

## **PUT request**

Related: **request**

## **PuTTY**

A Windows SSH and Telnet client. Pronounced “putty.”

## **pwdump**

A pen testing tool.

## **pwn** (v. or n.)

To defeat, to own. Pronounced “pown.”

## **The Pwnie Awards**

Annual awards for hackers.

## **Python**

A programming language. Monty Python references in tool names are encouraged.

Related: **spam, unpickling**

# Q

## **QA**

Short for Quality Assurance.  
Everyone needs an editor. :)

## **QLess**

A queue management platform.

## **QR code**

Quick response code. Do not spell out.

## **QSA**

Quality Security Assessor. Spell out on first use.

Related: **PCI**

## **query string**

## **queue** (n.)

## **QuickTime**

## **QWERTY**

A common keyboard layout originally designed for typewriters.

Related: **Dvorak**

# R

## **race condition** (n.)

## **rainbow table**

Related: **decryption, encryption**

## **RAM**

Random access memory. Do not spell out.

## **RankBrain**

A Google AI algorithm that helps to sort search results.

## **ransomware**

Malware that threatens to publish or delete data unless a ransom is paid.

## **RAR file, .rar file**

Related: **file extensions**

## **Raspberry Pi**

A single-board computer. Versions include Raspberry Pi 3 model B and Raspberry Pi Zero W.

Related: **Danger Drone**

## **RAT**

Remote access trojan. Spell out on first use.

## **rate-limit** (v.), **rate limiting** (n.)

**ratios**

Write with a colon and no space as in "32:9."

Related: **numbers, pixel**

**RBA**

Risk-based assessment. Spell out on first use.

**RC4 NOMORE**

An attack that affects the RC4 cipher. RC4 is pronounced as letters or "ark-four."

**RCE**

Short for remote code execution. Spell out on first use.

**rcp**

Short for remote copy. Allows the transfer of files to and from another system over the network.

**RCPT**

Short for receipt. A verb in SMTP.

**RDP**

Remote Desktop Protocol.

**RDS**

Relational Database Service. Spell out on first use.

**read access****readme file** or **README file****read-only** (adj.)**read/write** (adj.)

As in "read/write privileges."

**real-time** (adj.), **in real time** (n.)**reCAPTCHA, reCAPTCHAs**

Google's proprietary CAPTCHA system.

**[REDACTED]**

Indicates a censored section of code, often passwords or PII.

**Reddit, redditor**

Related: **subreddit, upvote**

**Red Hat**

Linux operating system.

**Redis**

An open source in-memory key value store.

**RedLock**

A Cloud DevOps vendor.

**RedSnarf**

A pen testing tool.

**red team, red teaming**

Red teaming can mean many things in an assessment. Define briefly on first use to clarify your intended meaning.

**RedTube**

Related: **Pornhub, Rule 34**

**reduce** (v.)

To lower the likelihood of an attack. Not synonymous with "mitigate," which lessens the severity of an attack.

**Referer**

Famously misspelled HTTP header.

**reflect** (v.), **reflected** (adj.)

An attack pattern in which a payload is copied verbatim onto a victim's context.

**regex**

Regular expression. Pronounced “redge-X” or “regg-X.”

**registry hive****remediation** (n.), **remediated** (adj.)

The process of improving a system to a known good state in which elements of a vulnerability or impact have been eliminated.

**remote access** (n.)**remote desktop** (v.)**replay attacks****replicants**

Fictional androids in 1982’s Blade Runner.

**reportlet, reportlets****report names**

If referring to a report in general, capitalize as in “the July 2017 Remediation Report.” If referring to the specific filename or path, use tech font.

**reproducible** (adj.)**requests**

Capitalize all types of requests and use normal font.

Ex: [GET request](#), [pull request](#)

**response-splitting****REST, RESTful**

Web services.

**retcon** (v. or n.)

Informal. To retroactively change the continuity of a story in a “do-over.”

**retest** (v. or n.)

As in “this finding was not retested.”

**retweet** (v. or n.)

Related: **hashtag**, **RT**, **Twitter**

**reuse** (v. or n.)**reverse-engineer** (v.)**reverse engineering** (n.)**reverse proxy** (n.)**reexec**

Short for remote execute. Pronounced “R-exec.”

**RFB**

The Remote Frame Buffer protocol.

**RFC 1149**

A Standard for the Transmission of IP Datagrams on Avian Carriers: “Avian carriers can provide high delay, low throughput, and low altitude service.”

**RFC 1918**

The Request for Comment 1918 memorandum assigns private IP addresses.

**RFID card**

Radio frequency identification card.

**RFP**

A request for proposal. Spell out on first use in public-facing documents.

## **Rickmote Controller**

A rickrolling remote control created by BF's own Dan "AltF4" Petro in 2014.

## **rickroll (v.), rickrolling (n.)**

Related: **4chan**, **meme**

## **ride-share, ride-sharing**

## **right-click (v.)**

## **ringtone**

## **RISC**

Reduced instruction set computing.  
Architecture used in some microprocessors.

## **risk**

The perceived threat of a security weakness based on the business impact, likelihood of exploitation, and cost to mitigate or reduce the threat.

## **RMI**

Short for remote method invocation. Spell out on first use.  
Related: **JMX**, **JVM**

## **RNGs**

Random number generators.

## **roadblock**

## **roadmap**

## **ROBOT attack**

Return of Bleichenbacher's Oracle Threat.

## **rogue access point**

Related: **Stingray**

## **rogue cell tower**

Also called a "cell-site simulator."

## **root or root**

Use the tech font when referring to a specific root account or user. Use regular font when referring to a more general instance, such as the root of an XML document or a web root.

## **rootkit (n.)**

## **Root the Box**

An annual CTF competition and its supporting software infrastructure.

## **ROP**

Return-oriented programming. Spell out on first use.

## **RoR**

The Ruby on Rails web application framework. Spell out on first use.

## **RPC**

Remote procedure call.

## **RPG**

Role-playing game.

## **RSA**

A tech company, an annual San Francisco security convention, and an encryption algorithm. RSA stands for the last names of the 3 co-founders. Do not spell it out.  
<https://www.rsaconference.com/>

## rsh

Short for remote shell. Allows the execution of non-interactive programs on another system.

## RSS feed

Rich Site Summary. Do not spell out.

## RT, RT'd, RTs

Retweets on Twitter.

## RTFM

Read the fucking manual.

Related: **tl;dr**

## Rubber Ducky

Related: **USB Rubber Ducky**

## Ruby

A programming language.

Related: **RoR**

## Rule 34

If it exists, there is porn of it.

Related: **Pornhub, RedTube**

## rulesets

## runas

A command to execute a program by "running as" another user.

## runtime (n.), run-time (adj.)

The common language [runtime](#). The [runtime](#) of Blade Runner. A [run-time](#) function or analytic. [Run-time](#) errors.

# S

## S3, S3 buckets

Short for Simple Storage Service. An Amazon service.

## SaaS

Software as a service. Pronounced "sass."

Spell out on first use.

Related: **IaaS, KMaas, PaaS**

## safelist, safelisting

A proposed alternative term to whitelisting.

Not yet widespread.

Related: **blocklist**

## Salesforce

## salami slicing attack

Repeatedly stealing money in very small quantities.

Related: **bitcoin, cryptocurrency**

## salt (v. or n.), salted (adj.)

In encryption, salted code has random values sprinkled in it to make it more difficult to decode. If two users have the same password, salting ensures that their hashes won't be the same.

## same-origin policy (SOP)

Spell out on first use.

## SAM file

Sequence alignment format file.

## **SAML**

Short for security assertion markup language. A programming language. SAML rhymes with camel.  
Related: **a** vs. **an**

## **sandbox environment, sandboxing**

### **sandbox escape**

Modifying privileges in a system past the manufacturer's intention in order to gain root access. More generic than "jailbreak."

### **sanitized** (adj.)

## **SANS**

The SysAdmin Audit Network Security Institute. Pronounced "sans."

## **Scala**

Programming language meant to address criticisms of Java.

### **scannability** (n.), **scannable** (adj.)

## **SCCM**

System center configuration manager. Spell out on first use.

## **Schannel**

Short for Secure Channel. A Windows SSP.

### **science fiction** or **sci-fi**

Related: **AI**, **android**, **Aperture Science**, **cyberpunk**, **Cylon**, **deus ex machina**, **FTL**, **grey goo**, **hyperspace**, **nanotechnology**, **Skynet**, **The Three Laws of Robotics**, **uncanny valley**

## **scope**

The list of applications and environments that a pen testing team tests for vulnerabilities during an engagement.

### **scope creep** (n.)

### **</scorpion>**

An inaccurate CBS TV show about hacking.

### **scrape** (v.), **scraping**

A script can retrieve (scrape) all of the data from a webpage in lieu of an API retrieving the specifically desired information.

### **screencap, screenshot**

We don't use these terms in formal writing unless the method of capture is relevant to the narrative.

### **screen-capture** (v.)

### **screensaver**

### **script, scripting**

### **script code**

### **scroll bar**

### **scrum**

An Agile framework. Also the name of meetings within that system.  
Related: **Agile**, **sprint**

### **scrypt**

A hashing (not encryption) algorithm. Pronounced "ess-crypt."

**SCSI**

Short for Small Computer System Interface. A parallel interface. Pronounced “skuzzy.”

**SDK**

Software development kit. Spell out on first use.

**SDLC**

Software development lifecycle. Spell out on first use.

**SDN**

Software-defined networking. Spell out on first use.

**sealioning (n.)**

A type of trolling that involves persistently asking questions in bad faith.

**second-order (adj.)**

As in “second-order SQL injection.”

**secure boot (n.)****security breach (n.)****security controls**

Code and other tools (as opposed to policy) that enforce repeatable security. There are preventative controls, detective controls, and corrective controls.

**Security Conversations**

A Bishop Fox podcast.

**security key (n.)****Security Monkey**

AWS configuration monitoring.

**security question**

Use normal font with quotation marks around questions as in “What was the name of your favorite unpaid internship?”

Related: **error message**

**security through obscurity**

The rightly maligned practice of making a system extremely complex in the hope that it will prevent anyone from figuring out how to hack it.

Related: **principle of least privilege**

**Security Without Borders**

A collective of industry volunteers who help others solve cybersecurity issues.

<https://securitywithoutborders.org/>

**seed (n. or v.), seeding****segregate (v.), segregation (n.)**

Do not use. When referring to splitting up network parts, use “segment” or “separate.”

**segue (n.)****Segway****SegWit**

Cryptocurrency term. Segregated Witness.

Related: **network segmentation**

**self-driving vehicle (n.)****self-generated (adj.)****selfie stick (n.)****SEO**

Search engine optimization. Spell out on first use.

## **serialization**

### **server**

Write names or types of servers in normal font as in "SMTP server."

### **server-side** (adj.)

### **ServerSignature**

### **ServerTokens**

### **service provider**

### **servlet, servlets**

### **servo, servos**

### **session fixation**

### **set up** (v.), **setup** (n. or adj.)

### **SHA-1, SHA256**

Secure Hash Algorithm.

### **SharePoint**

A Microsoft product.

### **sharing economy**

Related: **Airbnb**, **Kickstarter**, **ride-share**

### **shell**

You can gain, get, pop, spawn, or drop a shell. Use "persistent remote access" in formal writing to explain the threat of shells to clients.

Related: **shell script**

### **shell script**

Related: **reverse shell**, **root shell**, **webshell**

## **Shellshock**

A GNU Bash vulnerability. Also known as Bashdoor.

### **shelve** (v.)

To discontinue the use of.

## **Shodan**

### **short-name**

A shortened filename. Also called an 8.3 filename.

### **short-term** (adj.)

### **shoulder surfing**

Standing behind someone to steal their password, etc.

### **-side**

Always hyphenate in adjectives.

Ex: **client-side**, **server-side**

## **SIEM**

Security information and event management. Pronounced "sim." Spell out on first use.

## **Signal**

A private messaging app.

Related: **WhatsApp**

### **signal-to-noise ratio**

### **signature** (n. or v.)

Avoid as a verb if possible. Try "identify" instead.

### **signed long** (n.)

A long signed integer type of C data.

**sign in (v.), sign-in (n.)**

**sign out (v.), sign-out (n.)**

**sign up (v.), signup (n.)**

### **Silicon Valley**

A generic term for the tech industry based in the greater San Francisco Bay Area. Also the name of an HBO TV show about a startup company called Pied Piper.

### **Silk Road**

A black market website that was operational between 2011 and 2014.

**silos, siloed (v.)**

**silos, silos (n.)**

### **SIM card**

### **the singularity**

Related: **AI, grey goo, Moore's Law**

**sinkholing (n.)**

Traffic redirection.

### **SIP**

Session Initiation Protocol. Spell out on first use.

### **Siri**

Apple AI.

Related: **Alexa, Cortana, Google Assistant**

### **SIR Plan**

Security incident response plan. Spell out on first use.

### **Sitecore**

### **site map**

### **Six Sigma**

**skeuomorph (n.)**

A modern feature that is styled to look like an older, physical version. For example: the floppy disk Save button or the shopping cart icon used by online retailers.

### **skill set**

Related: **soft skills**

### **Skynet**

The fictional AI tech by Cyberdyne Systems that led to the creation of the Terminator.

Related: **AI, sci-fi**

### **SLA, SLAs**

Service-level agreement. Spell out on first use.

### **SLAAC attack**

Stateless Address Autoconfiguration.

### **Slack**

A group messaging system.

Related: **IRC**

**slash or /**

Related: **characters**

**slideshow (n.)**

### **slug**

A user-friendly URL.

### **smartglasses**

### **smart lock**

A generic term for an IoT lock.

**smartphone**

An internet-enabled cell phone.

**smart safe****smartwatch****SmashBot**

The unbeatable Nintendo Super Smash Bros. AI created by BF's own Dan "AltF4 Petro.

**SMB**

Server Message Block. Spell out on first use.

**SMEs**

Subject matter experts. Spell out on first use.

**S/MIME**

Public encryption key standard for MIME data.

**SMS**

Short message service.

**SMTP server**

Simple Mail Transfer Protocol.

**sniff (v.)**

To monitor and capture data packets that pass through a network.

**snippet**

An amount of quoted code. In formal writing, we use "a code excerpt" instead.

**SNMP**

Simple network management protocol.

**SNMPwalk**

A network monitoring tool.

**Snyk**

An open source security tools company. Pronounced "sneak" or "snick."

**S/O or s/o**

Informal. Short for shout out. A way to publicly thank someone online.

**SOA**

Short for Start of Authority or service-oriented architecture. Spell out on first use.

**SOAP**

Simple object access protocol. Spell out on first use.

**SoC**

System on chip. Spell out on first use.

**social engineering**

Related: **cold-call, phishing, pretexting, RFID card, spoof, tailgating, trick**

**social media**

Related: **emoji, Instagram, Like, Reddit, Snapchat, Twitter, upvote, Web 2.0**

**Social Security number (SSN)****socket**

For types of socket, use normal font. For a specific socket, put the socket type in tech font as in `jmxrxi` socket.

**SOCKS**

Socket Secure protocol.

**Sofacy**

A hacking group also known as APT28 or Fancy Bear.

**soft skills**

In contrast to hard programming skills, these are skills like listening, presenting, and personal networking.

**soft token****software**

Related: **-ware**

**software piracy** (n.)**solid state** (adj.)

SSD is short for solid state drive.

**SomaFM**

DEF CON radio. <https://somafm.com/>

**SOP**

Same-origin policy. Spell out on first use.

**source code****SOW**

Statement of Work. Spell out on first use.

**spacebar****SpaceX****spam** (v. or n.)**spear-phishing** (n. or v.)

Tailored phishing attacks aimed at a specific target.

**-specific** (adj.)

Always hyphenate.

Ex: [client-specific](#), [task-specific](#)

**Spectre**

A flaw that affects Intel, AMD, and ARM chipsets. It was publicly disclosed in January 2018. The James Bond supervillain organization is SPECTRE.

Related: **Meltdown**

**speedrun, speedrunning****SpEL**

Spring Expression Language.

**spellcheck** (v.), **spell check** (n.)

Related: **Cupertino effect**

**SPF**

Sender Policy Framework. Spell out on first use.

**sphere of control****splash page****split tunneling****Splunk**

A security tool, a SIEM.

**spoof** (v. or n.), **spoofing** (n.)

To create a fraudulent, attacker-controlled replica of legitimate data like a website.

Related: **phishing**

## **SpoofCheck**

A Bishop Fox tool by Alex DeFreese that determines if an email or domain has either DMARC or DKIM email protections.  
<http://spooftcheck.bishopfox.com/>

## **Spring Framework**

A Java application framework.

## **sprint**

Related: **Agile, scrum**

## **spyware**

## **SQL**

A programming language. Precede with "a," assuming that the reader pronounces it as "sequel." Sometimes pronounced as letters.  
Related: **a** vs. **an**

## **SQLi**

The SQL injection application vulnerability.  
Pronounce the phrase or "sequel-eye."

## **sqlmap**

A tool that finds and exploits SQL injections.

## **Square Cash**

A mobile payment service.  
Related: **PayPal, Venmo**

## **Squarespace**

## **Squid**

A web proxy.

## **SSD**

Short for solid state drive. A drive with no moving parts. Spell out on first use.

## **SSDLC**

Secure software development lifecycle.  
Spell out on first use.

## **SSHD**

Solid state hybrid drive. Spell out on first use.

## **SSH port**

The Secure Shell protocol.

## **SSI**

Server Side Includes.

## **SSID**

Service Set Identifier. The human-readable name of a Wi-Fi network. Spell out on first use.

## **SSL Labs**

## **SSL/TLS**

Security protocols. Secure Sockets Layer/Transport Layer Security.

## **SSN**

Short for Social Security number. Don't capitalize "number." Spell out on first use.  
Related: **ATM, PIN**

## **SSO**

Single sign-on. Spell out on first use.

## **SSP**

Security support provider. Spell out on first use.

## **stack canaries**

## **stack trace**

## staff augmentation

### stageless (adj.)

As in “stageless Meterpreter payload.”

## stakeholder

### start up (v.), startup (adj. or n.)

Start up the laptop. A startup company.

### stateless (adj.)

HTTP is a stateless protocol.

## status, statuses

## Steam

A video game distribution platform.

## steganography

A strategy of hiding information to avoid its capture rather than openly disguising it through cryptography.

## sticky cookie

## Stingray

A surveillance tool that appears as a Wi-Fi network but actually takes information from the devices that connect to it.

Related: **rogue tower**

## STIX

Structured Threat Information Expression.

## stockholder

## stream, streaming

Related: **livestreaming, OTA**

## The Streisand Effect

The effect states that requesting the internet to not do something will cause the internet to deliberately do that thing more.

### string literal (n.)

A string of characters written directly into the code.

### strong (adj.)

## Stuxnet

A worm that sabotaged Iranian uranium enrichment in 2010.

## su

Short for superuser. Use tech font as in “su command.”

Related: **sudo**

## subdirectory

## subdomain

## subkey

## subnet

## subreddit

## subsection

## subsystems

### subtweet (n., v.)

### subvert (v.)

## sudo

Superuser do.

Related: **su**

## **sudoer**

Someone who has sudo privileges. In formal writing, try “user with sudo privileges” if it’s not part of a set expression.

## **sunset (v.)**

Business jargon for planned phasing out. OK to use sparingly in the infinitive. Also try “no longer support” or “decommission.”

## **superclass**

If writing about a type of superclass, use normal font. If it’s the name of a superclass, use tech font as in `Throwable`.

## **SuperHappyDevHouse (SHDH)**

A type of hackathon party.

## **superuser**

## **surveillance software**

## **SVN**

Subversion.

## **Swagger**

Tools for implementing OpenAPI.

## **sweepstakes (n.)**

## **Sweet32 attack**

## **SWF file, .swf file**

Pronounced “swiff.”

Related: **file extensions**

## **Symfony**

A PHP framework.

## **sync (n. or v.), syncing (v. or adj.)**

## **sysadmin user**

## **syslog server**

## **system**

If writing about a specific system, use tech font as in “`dev_test` system.” Otherwise, use normal font.

## **systematically**

## **systemic, systemically**

## **system on chip (SoC)**

Spell out on first use.

# **T**

## **table-top modeling**

Related: **blue teaming**, **threat modeling**

## **tag stripping**

## **tailgating**

Entering a secure area by tagging along with someone who has the proper credentials.

## **tail of the file**

The last 10 lines of a file. Can be requested through the command `tail`.

## **tailor (v.)**

Also “hone” or “refine.”

## **take over (v.), takeover (n.)**

An attacker could **take over** the system. It was a complete system **takeover**.

## **target, target system**

Related: **red teaming, trophy**

## **tarpitting (n.)**

The deliberate slowdown of a network to contain or deter an attack.

## **Tastic RFID Thief**

A Bishop Fox tool that can copy RFID credentials up to three feet away.

## **TCP/IP**

Short for Transmission control protocol/internet protocol. Wired Style calls it “the mother tongue of the internet.”

Related: **UDP**

## **tech-savvy (adj.)**

## **Tectia SSH**

## **TED Talks and TEDx[city]**

Short for technology, entertainment, and design. Global nerd conferences. Do not spell out.

## **TEE model**

Short for Trusted Execution Environment. A co-processor on ARM (found on Android).

## **Telemetry API**

## **telephony pen testing**

Related: **social engineering**

## **teleprompter**

## **Telnet**

A remote login protocol.

## **test bed**

## **text box**

## **text message**

## **tgrep**

Pronounced t-grep.

Related: **grep, ngrep**

## **they**

Use singular they. As with all language, be mindful of possible clarity issues.

## **thick client**

A computer that provides rich functionality independent of the server. Also called a fat client; don't use “fat client” in formal writing.

## **thin client**

The opposite of a thick client.

## **third party (n.), third-party (adj.)**

An external party like a vendor that exists outside of the company-user relationship.

## **threat, threats**

Security threat categories include competitor, hacktivist, insider, dealer, nation state, and third-party integrator.

## **threat hunting**

Defensive security.

Related: **blue team**

## **threat modeling**

Exercises that run through risk assessment procedures or incident response plans. Also called table-top modeling.

## The Three Laws of Robotics

Written by Isaac Asimov. "1: A robot may not injure a human being or, through inaction, allow a human being to come to harm. 2: A robot must obey orders given to it by human beings except where such orders would conflict with the First Law. 3: A robot must protect its own existence as long as such protection does not conflict with the First or Second Law."

## throughout

### throughput (n.)

The total amount of data transmitted over a link per unit of time.

Related: **badput**, **goodput**

### throw, threw (v.), thrown (adj.)

When the code throws an error, it announces that something is wrong that the code cannot fix. Thrown errors can be "caught" by other portions of code.

## Throwable

### tikzpeople

LaTeX emoji.

## tilde enumeration

Tilde is the [~] character used in coding and the Spanish ñ.

### time-boxed (adj.)

Describes engagements that are limited by scoped hours.

### timeframe (n.)

### time-lapse (adj.)

## timeline

### timeout (n.), time out (v.)

## timestamp

## time zone

## titles of published works

Titles of books, movies, podcasts, TV shows, and video games do not often appear in our formal writing. When they do, we write them in title case as in Snow Crash. If the title does not stand out on its own, add quotation marks, as in the dystopian novel "We" or the video game "E.T."

## TLAs

Three-letter agencies. Refers to government agencies like the CIA, FBI, and NSA. Informal.

## TLD, TLDs

Top-level domain. Spell out on first use.

## tl;dr or TL;DR

Too long; didn't read.

Related: **RTFM**

## TLS

Transport Layer Security. The replacement for Secure Sockets Layer (SSL).

## TOCTOU bug

Short for "time of check to time of use." A software issue that occurs between checking a condition and using the results of the check. Pronounced "tock-too." Related: **race condition**

## token

When discussing a type of token, use normal style as in "OAuth bearer token." If it's a specific token, use the tech font for the name only, unless it is linked to the word "token" as in "oauth\_token."

## toolbar

## toolchain

## Tor

Short for The Onion Router. A privacy-focused web browser. Don't write as TOR.  
Related: **I2P**, **.onion sites**

## torrent

## TOTP

Short for Time-based One-time Password. An algorithm. Spell out on first use.  
Related: **HMAC**

## touchpad

## touchscreen (n. or adj.)

## tower defense

A genre of games in which the player builds defenses to survive wave after wave of enemy attackers.

## T-POC

Technical point of contact. Pronounced "tee-pock." Spell out on first use.  
Related: **PoC**

## traceback (adj. or n.)

## trapdoor

## trend line

## triage (n. or v.)

## trick (v.)

OK in social engineering engagements. Also consider **coerce**, **force**, or **prompt**.

## trigger (v.)

## trim range, trim value

Related: **denial of service**

## trivial (adj.)

If describing an easy-to-bypass security measure, choose a more descriptive word like insignificant, unsophisticated, or easily overcome. OK in the phrase "Although non-trivial to implement..."

## trojan

Malware that masquerades as something legitimate.

## troll (n. or v.), trolling (n.)

Hateful or intentionally ignorant behavior that intends to cause strong reactions and waste time. Don't feed the trolls.

Related: **4chan**, **dox**, **flame war**, **sealioning**, **The Streisand Effect**

## trophy

A prized target within an environment.

OK in formal writing if trophies have been established with the client.

Related: **red teaming**, **target**

## troubleshoot (v.)

## TrueCrypt

## **trust boundary**

## **T-SQL**

A programming language used by MS SQL Server.

## **TTD**

Time to detection. Spell out on first use.

## **TTP, TTPs**

Tactics, techniques, and procedures. Used during threat modeling exercises. Spell out on first use.

## **Tumblr**

## **TunnelBear VPN**

## **Turing Test**

Are you a robot? Let's find out.

## **Turla**

A hacking group also known as Snake or Uroburos.

## **tvOS**

## **TW**

Trigger warning. Spell out on first use in public-facing documents.

## **tweet, retweet** (v. or n.)

## **Twitter**

A microblogging website. Our account is @bishopfox.

Related: **hashtag, RT, subtweet**

## **Twitterstorm**

## **two-factor authentication (2FA) or (TFA)**

Related: **MFA**

# **U**

## **UDP**

User Datagram Protocol. A faster, more lossy alternative to TCP. I was going to tell you a UDP joke, but I'm afraid you might not get it.

## **UGT**

Universal Greeting Time. On IRC, it's always morning when you log on and always night when you log off.

## **UI** (n.)

User Interface.

## **uncanny valley**

The disturbing nightmare gap between semi-realistic artificial faces and actual living humans.

## **Unicode Consortium**

A nonprofit that decides internet standards for emoji and Unicode.

## **unicorn**

Business jargon for a successful startup. Do not use in formal writing.

Related: **BYOD, coworking space, crowdfund, sharing economy, startup**

## units of measurement

Pay attention to unit capitalization (GB, Gb, GiB. Don't pluralize units as in "500TB."

Don't put a space between the number and the unit for things like MB and GHz. Do use a space for some units like dpi, fps, and ms. Use the International System of Units (SI) for further guidance.

Related: **bps, bytes, dpi, GBps** vs. **Gbps, KB, KHz, MB, ms, numbers, pixel, p.m.**

## Unix or UNIX

An operating system. Not an acronym. Pronounced "you-nicks."

## unpickling

In Python, the process of taking something out of serialization.

## The Unreal Engine

### unremediated (adj.)

We prefer to write that "the issue was not remediated" to avoid implying that the problem was solved and then unsolved.

### unsanitized (adj.)

Means that security checks have not been performed. Typically pertains to user-supplied data. "Sanitized" data should be safe for an application to ingest, whereas unsanitized data may not be.

### unserialize (v.), unserialized (adj.)

## Untwister

A tool that predicts random numbers from insecure algorithms.

## unvalidated vs. invalidated

**Invalidated** data has been checked and deemed invalid. **Unvalidated** data has not been checked at all.

### upload (v. or n.)

The opposite of download.

### uppercase (adj. or v.)

Better to write "put in uppercase" but if needed, "uppercased" is OK.

## UPS

Uninterruptible power supply. Spell out on first use.

## uptime

The opposite of downtime.

### up-to-date (adj.)

### upvote (v. or n.)

Term used to approve stories on Reddit. Analogous to a Facebook "like."

## URI

Uniform/Universal Resource Identifier. Both URLs and URNs are subsets of URIs. Use tech font.

Related: **data:**

## URL

Uniform/Universal Resource Locator. Use tech font for URLs (including IPv6). Avoid starting sentences with URLs. Write variable segments in bold color as in `zombo.com/[variable]`.

Related: **.NET Framework**

**URL-encoded** (adj.), **URL encoding** (n.)

A specific kind of encoding used by browsers for characters outside the ASCII set and certain other characters (e.g., spaces and ampersands).

**UrlScan**

A Microsoft application.

**URL shortener, URL-shortening****URN**

Uniform/Universal Resource Name.

Related: **URI**

**USB drive**

A storage device that connects via USB. A small form-factor USB drive is a thumb drive. A flash drive is any drive with Flash memory (solid state/NAND or USB).

**USB Rubber Ducky**

A keyboard HID that automates keystrokes. Rubber Ducky is OK on second use.

**use after free** (n.), **use-after-free** (adj.)

A vulnerability.

**Usenet**

A bulletin board system that preceded the modern internet and still exists.

**user base** (n.)**username**

Write usernames in the tech font as in admin or Zero Cool.

**user-supplied** (adj.)**UTF-8**

A Unicode character encoding. (Don't pronounce the dash).

**UX**

User experience. Spell out on first use.

# V

**value**

If writing about a type of value, use normal font. If it's a specific value, use tech font as in "LicenseID value."

**VBScript**

A Microsoft programming language.

**VDI**

Virtual desktop infrastructure. Spell out on first use.

**vendor**

A third-party business that provides a service to a client.

**Venmo**

A mobile payment service.

Related: **PayPal, Square Cash**

**VeraCrypt**

Disk encryption software.

**verbose** (adj.)

Verbose logs, banners, and error messages reveal more information about underlying structures to users and attackers than is necessary.

**verb tunneling (n.)**

**version numbers**

Use normal font for software version numbers, product model numbers, serial numbers, and builds.

**VGA**

Video graphics array.

**via**

**victim**

Better to say user, patient, customer, or consumer, but this is OK sparingly.

**videoconference, videoconferencing**

Related: **audio conference**

**video games**

Capitalize video game titles in normal font as in *Myst* and *Grim Fandango*.

Related: **8-bit, FPS, Game Boy, GameCube, game jam, GaymerX, motion capture, Nintendo Switch, PAX, PlayStation, RPG, SmashBot, speedrun, Steam, titles of published works, tower defense, Wii, Xbox**

**Vim**

A text editor.

**Vimeo**

A video-sharing company.

**viral (adj.)**

**virtual reality (VR)**

**VLAN**

Virtual local area network. Pronounced “vee-lan.”

**VLCM**

Vulnerability Lifecycle Management. Spell out on first use.

**vlog**

**VM**

Virtual machine. Spell out on first use in public-facing documents.

**VMware**

**VNC**

Virtual Network Computing. Spell out on first use.

**voicemail**

**VoIP**

Voice over Internet Protocol. Pronounced “voyp.”

**VPC**

Virtual private cloud. Spell out on first use.

**VPN**

A virtual private network. Spell out on first use.

**VR**

Virtual reality.

Related: **AR, Oculus Rift**

**VSA**

A vendor security assessment. Spell out on first use.

## **Vuforia**

An AR platform.

## **vulnerability** or **vuln** (n.)

Any condition, configuration, or state that increases an asset's logical, informational, or physical exposure to loss of availability, integrity, or confidentiality. Vuln is informal.

## **vulnerability scan**

An assessment of a target using vulnerability-scanning tools to detect security weaknesses.

## **vulnerability scanner**

An automated application or system designed to assess computers, computer systems, networks, or applications for weaknesses.

## **vulnerable** (adj.)

# W

## **WAF, WAFs**

Web application firewall. Pronounced as "waff." Spell out on first use.

## **WAMP**

Short for Windows, Apache, MySQL, and PHP, which were its original four components. A software bundle. Do not spell out.

## **WampServer**

## **WAN**

Wide area network.

Related: **LAN**

## **WannaCry**

A ransomware attack that hit in May 2017.

## **war-dialing** (n.)

## **war-driving** (n.)

## **-ware** (n.)

Always close -ware compounds.

Ex: [bloatware](#), [freeware](#), [malware](#), [vaporware](#), [VMware](#), [WarioWare](#)

## **WarGames**

A 1983 movie about a NORAD AI that wants to play a game of thermonuclear war.

## **war gaming**

Also known as threat modeling or table-top gaming, e.g., capture the flag (CTF) at a security conference.

## **wasm**

WebAssembly. Pronounced "wass-im."

## **watch list** (n.)

## **watermark** (n. or v.)

## **Watson**

An IBM productized question-answering AI, famous for winning Jeopardy!

## **Web 2.0**

## **web app**

## **web application**

**web-based** (adj.)

**web browser**

Also just “browser.”

Related: **Chrome, IE, Mozilla Firefox, Tor**

**webcam**

**webcomic**

**web console**

**WebDAV**

Web Distributed Authoring and Versioning.

**web directory**

**web forum**

**webhooks**

User-defined HTTP callbacks.

**webinar**

**web page**

**web proxy**

**web root**

**web server**

**webshell**

**website** or **site**

Related: **homepage, portal, splash page, Squarespace, TLD, WordPress**

**WebSocket, WebSocket Protocol**

**WebSphere**

An IBM product.

**webtree** or **web tree**

Use “directory structure” instead.

**WebView**

An Android system component.

**weeklong** (adj.)

**well-formed** (adj.)

**Wget**

A GNU tool. Pronounced “W-get.”

**WhatsApp**

A messaging app.

**white-box testing**

**WhiteHat**

A company that makes a vulnerability scanner and supporting services.

**white hat**

**whitelist** (v.) **white list** (n.)

Related: **safelist**

**white space**

**whoami**

A command to identify the user.

**whois command, WHOIS database**

A query protocol.

**whole disk encryption**

**-wide** (adj.)

Always hyphenate.

Ex: [company-wide](#), [system-wide](#)

**widescreen** (n. or adj.)**widget**

If it's the name of a specific widget, write it in tech font as in Video widget.

**WIDS**

Wireless intrusion detection system. Spell out on first use.

**Wi-Fi**

According to the Wi-Fi Alliance, Wi-Fi does not stand for wireless fidelity. Do not write as WiFi or wifi.

**WiFi Pineapple****Wii****wiki** (n.)

A collaborative, editable blog.

**WikiLeaks****Wikipedia**

A user-curated online encyclopedia. Sometimes the findings we disclose are so new that the best resources on the topic are Wikipedia articles.

**wildcards**

Wildcard characters like [\*] and [%3f] can either stand in for a single character or a string of characters.

Related: **metacharacters**

**Windows**

Microsoft OS.

**Windows Registry****WinSCP**

Short for Windows Secure Copy. A Windows SFTP and FTP client.

**wireless signal bleed** (n.)**Wireshark**

A listening tool.

**wiretap** (n. or v.)**WOPR**

The fictional NORAD AI featured in the 1983 movie WarGames.

**WordPress****word processor****workflow****work stream****world-readable** (adj.)

Describes files or directories that any user could read.

**world-writable** (adj.)

Describes files or directories that any user could write to.

**WPA**

Wi-Fi Protected Access.

**write-only** (adj.)

## **WSDL file, .wsdl file**

Pronounced wazz-dull.

## **www**

The World Wide Web.

Related: **http://**

## **WYSIWYG**

Short for what you see is what you get.

Pronounced "wizzy-wig."

# **X**

## **x86**

## **Xbox**

## **xDedic**

An RDP tool.

## **XHR**

An XML HTTP request.

## **XLSX file, .xlsx file**

An XML-based spreadsheet file.

## **XML file, .xml file**

XML is short for extensible markup language. Use "an" before "XML file."

Related: **a vs. an, file extensions**

## **XOR encryption**

Short for exclusive or. Pronounced "exor."

## **Xpp3**

An XML parser.

## **XSS**

Short for cross-site scripting. Write as "an XSS" to reflect the way it's spoken. Spell out on first use.

## **XXE**

An XML external entity. Spell out on first use.

# **Y**

## **YA...**

Short for "Yet Another." Yahoo! is YACC: Yet Another Compiler Compiler.

## **YAML**

Short for "YAML Ain't Markup Language." A human-readable serialization language. YAML is a recursive acronym.

## **YAWAST**

A pen testing tool.

## **year**

Use normal font. No apostrophes for plural years as in "from the 1980s." Use apostrophes for events from that year as in "1999's song of the summer." Use a comma between day and year as in "July 4, 2000."

## **Yemen Cyber Army**

A hacking group that may be Iranian.  
Related: **false flag**

## **YML file, .yml file**

Related: **file extensions**

## **YouTube**

## **YubiKey**

A hardware authentication device.  
Pronounced "you-bee-key,"

## **YUM**

A Linux software update mechanism.  
Yellowdog Updater Modified.

# **Z**

## **zero-day** (n. or adj.)

A vulnerability that has been publicly known for zero days as in "zero-day attacks." In formal settings, use "publicly undisclosed vulnerability" or "previously undisclosed vulnerability."

## **zero growth model**

## **ZIP archive**

## **ZIP code**

## **ZIP file, .zip file**

Related: **file extensions**

---

# APPENDIX A: DECISION-MAKING NOTES

## How We Choose Our Terms

Three guiding principles help us decide which terms to use and how to write them:

### 1. We need to be accurate.

- Our readers need to understand the findings in our reports so that they can implement our recommendations. We live and breathe information security, so we can deviate from non-industry authorities (like AP style) if their advice is outdated or too broad for our audience. Our terms should reflect the way that real attackers perceive and exploit systems.

### 2. We want to be consistent.

- Many hands touch every report. We want each finding to have the same voice, even if a team of seven collaborated on it. We engage with the same clients through multiple assessments, so we use terminology consistently to help give our reports a logical narrative that non-technical readers can follow as well.

### 3. We'd like to look good at the same time.

- Beautiful documents are inviting and easier to read. We amplify the quality of our technical work through the look and feel of our reports. We use structural clarity and white space to give our dense technical information some room to breathe.

These principles are listed in order of priority. Sometimes we deliver reports that are accurate and internally consistent that do not line up with previous reports. We aspire to align our vocabulary with the most current and sustainable standards, but deadlines and custom engagements require us to find a balance between speed and perfection.

This prioritization also means that when punctuation and spacing are crucial to the technical understanding of a certain code snippet or URL, we choose to make things look accurate rather than stylish.

---

#### EXAMPLE: THE NONBREAKING HYPHEN

An editor might suggest using the nonbreaking hyphen to condense a long URL down from four lines to two. However, clients may directly copy our report text into Terminal or a text editor where the standard hyphen [-] and the nonbreaking hyphen [-] are two separate Unicode characters. Replacing one with the other would alter the sequence and make the finding unreproducible, so we keep the URL as is. It's not as pretty, but it is functional.

## How To Codify Your Own Terms

Sometimes capitalization matters. Sometimes spacing matters. Sometimes punctuation matters. Often, they matter for different reasons in code and in prose writing. Together, we make the Bishop Fox style work for all parties. To codify a new term for your own use, determine the following:

- Which type of font should be used?
  - fixed-width (monospace) or variable width font
- How is the term capitalized by its creators and its users?
  - Ex: [BeEF](#), [iPhone](#), [JavaScript](#), [Metasploit](#), [PuTTY](#), [QWERTY](#)
- If it's an acronym, how is it pronounced by its creators and its users?
  - Ex: [SQL](#), [ngrep](#), [Hping](#), [NAND](#)
- If it's an acronym, should its components be written out on first usage or never?
  - Ex: [3G](#), [APT](#), [IP](#), [RSA](#)
- Can it be confused with another term? If so, how to consistently distinguish?
  - Ex: [crypto](#), [fingerprints](#), [MFA](#), [shell](#)
- If it's a compound, how it is written as a noun vs. an adjective?
  - Do spacing/hyphens change the meaning or is it a personal preference?  
If it's a personal preference, decide a company-wide preference.

In the likely event that you find a term or phrase that is written or pronounced inconsistently, contact the creators and follow their preference. If that's not possible, check their most recent documentation. Ultimately, make a choice and use it consistently, but be willing to revise your answer in the future.

## How To Write Terms That Don't Follow Your Style

If a client uses a spelling other than the one we use, we make a choice depending on the situation:

1. If it's a typo in the quoted code, leave it as is.
2. If directly referring to a product name or heading in their environment, spell and capitalize it their way, as in [E-mail Address](#). Sometimes we also put the term inside quotation marks to separate its specific meaning from the generic term.
3. If we are referring to the generic term, we spell it our preferred way as in [email address](#). If examples in your code snippets or figures use the client's spelling, check to see if the spelling difference might confuse the reader or change the meaning. If you foresee a problem, talk to your editor.

---

## APPENDIX B: EXTERNAL RESOURCES

These resources can level up your security knowledge and technical writing skills. The sections below are divided into the following categories: our reference materials, technical definitions, internet-savvy style guides, writing advice, introductory hacking resources, security organizations and publications, and additional resources.

### Our Reference Materials

Associated Press. *The Associated Press Stylebook 2017 and Briefing on Media Law*. Revised, Updated edition. New York: Basic Books, 2017. <https://www.apstylebook.com/>

Editors of Webster's New World College Dictionaries. *Webster's New World College Dictionary*, Fifth Edition. New York: Houghton Mifflin Harcourt, 2016.

Microsoft Corporation. "User interface elements." In *Microsoft Manual of Style*. Page 93-98. Redmond: Microsoft Press, 2012.

### Technical Definitions and Explanations

"AWS in Plain English." ExpeditedSSL. Accessed February 9, 2018. <https://www.expeditedssl.com/aws-in-plain-english>

Begum, Farzana. "Becoming Acquainted with Bitcoin and Cryptocurrency Lingo." *BTCManager.com*. November 12, 2017. Accessed February 9, 2018. <https://btcmanager.com/becoming-acquainted-bitcoin-cryptocurrency-lingo/>

"CVE List Home." *Common Vulnerabilities and Exposures*. Accessed February 9, 2018. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12149>

"Glossary." OWASP. Updated February 11, 2017. Accessed February 9, 2018. <https://www.owasp.org/index.php/Category:Glossary>

"Glossary." Symantec. Accessed February 9, 2018. [https://www.symantec.com/security\\_response/glossary/](https://www.symantec.com/security_response/glossary/)

"Glossary of Key Information Security Terms." Edited by Kissel, Richard. NIST, May 2013. Accessed February 9, 2018. <http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf>

"Glossary of Security Terms." SANS. Accessed February 9, 2018. <https://www.sans.org/security-resources/glossary-of-terms/>

Newton, Harry with Steven Shoen. *Newton's Telecom Dictionary*, 30th Updated, Expanded Anniversary Edition. Telecom Publishing, Feb. 2016.

"PCMag Encyclopedia." PCMag. Accessed February 9, 2018.  
<https://www.pcmag.com/encyclopedia/index/a>

"researchtls and ssl cipher suites." *The Sprawl*. Accessed February 9, 2018.  
<https://www.thesprawl.org/research/tls-and-ssl-cipher-suites/>

"RFC 9494 – Internet Security Glossary, Version 2." The IETF Trust. Aug 2007. Accessed February 9, 2018. <https://tools.ietf.org/html/rfc4949>

"Threatasaurus: The A-Z of computer and data security threats." SOPHOS in collaboration with the Center for Internet Security, 2013. Accessed February 9, 2018.  
<https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf>

## **Internet-savvy Style Guides and Advice**

*Apple Style Guide*. July 2017 Apple, Inc. February 1, 2017. iBook.

Favilla, Emmy and Megan Paolone. *Buzzfeed Style Guide*. BuzzFeed, Inc. Accessed February 9, 2018.  
<https://www.buzzfeed.com/emmyf/buzzfeed-style-guide>

"Google Developer Documentation Style Guide." Google Developers. Updated June 8, 2017. Accessed February 9, 2018. <https://developers.google.com/style/>

*Hacker Dictionary*. Accessed February 9, 2018. <http://www.hacker-dictionary.com/terms>

Hale, Constance and Jessie Scanlon. *Wired Style: Principle of English Usage in the Digital Age*. New York: Broadway, 1997.

Hughes, Brianne. "Chaos in the Machine: Why Security Needs a Style Guide." Presented at CactusCon, Phoenix, AZ. Sept 29, 2017. Accessed February 9, 2018. <https://youtu.be/YL-4BWKpC28>

"The Jargon File." Version 4.4.7. Accessed February 9, 2018. <http://www.catb.org/jargon/html/>

Kopp, Rachel and Ganz, Steven. *Valley Speak: Deciphering the Jargon of Silicon Valley*. 2016. Genetius Publishing. May 17, 2016. <http://www.siliconvalleyspeak.com/>

"MailChimp Content Style Guide." MailChimp. 2017. Accessed February 9, 2018.  
<https://styleguide.mailchimp.com/>

PenzeyMoog, Caitlin and Laura M. Browning. "There are two e's in "Wookiee," damn it: A message from the A.V. Club copy desk." The A/V Club. Last updated December 18, 2015.  
<http://news.avclub.com/there-are-two-e-s-in-wookiee-damn-it-a-message-from-1798287457>

Sideways Dictionary. Accessed February 9, 2018. <https://sidewaysdictionary.com/#/>

soulaklabs. "Bitoduc.fr: termes informatiques en français." Accessed February 9, 2018. [bitoduc.fr](http://bitoduc.fr)

- A French and English hacker dictionary.

The tidyverse style guide. Accessed February 9, 2018. <http://style.tidyverse.org/index.html>

Wikipedia Manual of Style. Updated January 15, 2018. Accessed February 9, 2018.

[https://en.wikipedia.org/wiki/Wikipedia:Manual\\_of\\_Style](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style)

*Yahoo Style Guide: The Ultimate Sourcebook for Writing, Editing, and Creating Content for the Digital World.* Edited by Barr, Chris and the senior editors of Yahoo!. New York: St Martin's Griffin, 2010.

Yin, Karen. Conscious Style Guide. Accessed February 9, 2018. <http://consciousstyleguide.com/>

## Writing Advice

"Accessibility evaluation for web writers." *4 Syllables*. Accessed February 9, 2018.

<http://4syllables.com.au/articles/writers-accessibility-evaluation/>

Casagrande, June. *It Was The Best of Sentences, It Was the Worst of Sentences: A Writer's Guide to Crafting Killer Sentences.* New York: Ten Speed Press, 2010.

Clark, Roy Peter. *Writing Tools: 55 Essential Strategies for Every Writer.* New York: Little, Brown and Company, 2013.

Favilla, Emmy. *A World Without Whom: The Essential Guide to Language in the BuzzFeed Age.* New York: Bloomsbury, 2017.

## Introductory Hacking Resources

Clark, Ben. *RTFM: Red Team Field Manual.* 1.0 edition. CreateSpace Independent Publishing Platform, 2014.

Hak5. YouTube Channel. Accessed February 9, 2018. <http://www.youtube.com/hak5>

LiveOverflow. YouTube Channel. Accessed February 9, 2018. <https://liveoverflow.com/>

Paar, Cristof. "Introduction to Cryptography Lecture Series." YouTube Channel. 2010. Accessed February 9, 2018. <https://www.youtube.com/channel/UC1usFRN4LCMcfIV7UjHNUq/videos>

Stuttard, Dafydd and Marcus Pinto. *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws.* Indianapolis: John Wiley & Sons, Inc, 2011.

Sullivan, Bryan and Vincent Liu. *Web Application Security, A Beginners Guide.* McGraw Hill, 2001.

Yaworski, Peter. *Web Hacking 101: How to Make Money Hacking Ethically.* <https://leanpub.com/web-hacking-101>

## Security Organizations and Publications

"Blog." Bishop Fox. Accessed February 9, 2018. <https://www.bishopfox.com/blog/>

*Dark Reading*. Accessed February 9, 2018. <http://www.darkreading.com/>

*Electronic Frontier Foundation*. Accessed February 9, 2018. <https://www.eff.org/>

fdiskyou. "hacking Zines mirror for the lulz and nostalgia." Accessed February 9, 2018. <https://github.com/fdiskyou/Zines>

- A collection of historical hacking zines on GitHub.

Goldstein, Emmanuel. *The Best of 2600: A Hacker Odyssey*. Indianapolis: Wiley, 2008.

*Phrack Magazine*. Accessed February 9, 2018. <http://www.phrack.org/issues/69/1.html>

*Threatpost*. Accessed February 9, 2018. <https://threatpost.com/>

*We Live Security*. Accessed February 9, 2018. <https://www.welivesecurity.com/>

## Additional Resources

Bryan, Jenny. "How to name files." 2015. Accessed February 9, 2018. <https://speakerdeck.com/jennybc/how-to-name-files>

Hardikar, Aman. "Penetration Testing Practice Lab – Vulnerable Apps/Systems." Accessed February 9, 2018. <http://www.amanhardikar.com/mindmaps/Practice.html>

- A collection of pen testing resources.

InfoSec Conferences. Accessed February 9, 2018. <https://infosec-conferences.com/>

Kali Tools List. Accessed February 9, 2018. <http://tools.kali.org/tools-listing>

- A list of pen testing tools.

Know Your Meme. Literally Media, Ltd. Accessed February 9, 2018. [knowyourmeme.com](http://knowyourmeme.com)

"List of computer security certifications." *Wikipedia*. Updated January 6, 2018. Accessed February 9, 2018. [https://en.wikipedia.org/wiki/List\\_of\\_computer\\_security\\_certifications](https://en.wikipedia.org/wiki/List_of_computer_security_certifications)

Malware Unicorn Conference Search. Accessed February 9, 2018. <https://securedorg.github.io/community/search.html>

---

# EPILOGUE

## Muphry's Law

Murphy's Law says that anything that can go wrong will go wrong. Muphry's Law is an intentional misspelling of Murphy's Law that applies this buttered-side-down pessimism to writing and editing. Part of the law states that "any book devoted to editing or style will be internally inconsistent." If you find errors in this guide, or if you have ideas to improve the next version, please email [style@bishopfox.com](mailto:style@bishopfox.com).

Version 1	February 15, 2018	1,775 entries
Version 2	TBD	