

Internet Security 101

WHEATON PUBLIC LIBRARY

What is Malware?

Software designed to cause damage to data, devices, or the people using them.

Types of Malware

- **Virus:** Infects a specific document or software.
- **Worm:** Spreads by itself over a network.
- **Trojan horse:** Disguised as a legitimate program.
- **Spyware:** Tracks your internet activity to try and steal your information.
- **Ransomware:** Encrypts your files. Attacker will demand money to unlock them.
- **Adware:** Displays ads on your screen.
- **Rootkit:** Grants attacker remote access to your system.

Where Does Malware Come From?

- Visiting a compromised website
- Downloading infected files
- Using removable media (such as flash drives) which are already infected.
- Being connected to the same network as an infected computer.

Signs Your Computer May Be Infected

- Sudden increase in pop-up windows
- Change in homepage
- Sudden decrease in computer speed
- Frequent freezing or crashing

FREE Antivirus Software for Windows

- Avast (www.avast.com)*
- AVG (www.avg.com)*
- Windows Security (included with Windows 11)
 - ✓ Previously known as Windows Defender in Windows 10

*recommended by Consumer Reports

Top-Rated PAID Antivirus Software for Windows*

- Bitdefender (paid version) (www.bitdefender.com)
- AVG (paid version) (www.avg.com)
- ESET (www.eset.com)
- F-Secure SAFE (www.f-secure.com)
- Norton 360 Deluxe (www.norton.com)
- Avast (paid version) (www.avast.com)

*according to Consumer Reports (2021 data)

What about Kaspersky?

- Kaspersky (usa.kaspersky.com/) is a well-known and well-regarded antivirus software company.
- The FCC has added it to a list of companies that pose a threat to national security, and Consumer Reports has started including a disclaimer on their recommendation.
- It might be better to steer clear of this one for a bit.

Alert
 The Federal Communications Commission has added Kaspersky Lab, a Russian firm, to a list of companies it says pose a threat to national security. Previously, in 2015, Kaspersky Lab products were banned for use in federal computer systems. In addition, a number of independent security experts have expressed concern about the company. Consumer Reports has not independently tested Kaspersky Security Cloud Free for its vulnerability to exploitation by the Russian government.

Top-Rated FREE Antivirus Software for Mac*

- AVG (www.avg.com/en-us/avg-antivirus-for-mac)
- Avast (www.avast.com/en-us/free-mac-security)

*according to Consumer Reports (2021 data)

Top-Rated PAID Antivirus Software for Mac*

- Avast (avast.com)
- F-Secure SAFE (f-secure.com)
- ESET (www.eset.com)
- G Data (www.gdatasoftware.com)

*according to Consumer Reports (2021 data)

Firewalls

- Monitor all incoming & outgoing traffic and block anything unauthorized.
- A basic firewall is often included with your operating system.
- More comprehensive firewalls are available as standalone software or included with antivirus software.
- If you have multiple firewalls installed, disable all but one.

Web Browsers

Web Browsers

The software you use to connect to the Internet. Popular choices include:

-  Chrome (www.google.com/chrome)
-  Safari (included with Mac OS)
-  Edge (included with Windows 10 and 11)
-  Firefox (www.mozilla.org/en-US/firefox)





Web Browsers

- Whichever browser you choose, the most important thing to do is keep it updated.
- Use a pop-up blocker.

Browser Extensions

Browser installed apps that perform specific tasks for you. Can be used to get features your browser doesn't natively include.

Some examples of privacy-related extensions:

-  uBlock Origin (ublockorigin.com/)
-  Ghostery (www.ghostery.com)
-  Adblock Plus (www.adblockplus.org)
-  Privacy Badger (privacybadger.org/)

Passwords

Creating Strong Passwords

- Use 12-14 characters minimum (longer is better)
- Use a combination of uppercase and lowercase letters
- Include numbers and symbols

UNCOMMON (NON-GIBBERISH) BASE WORD ORDER UNKNOWN

Tr0ub4dor&3

CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO PROTECT FOR THE REST OF THE TIME BY TAKING ONE OF A FEW COMMON DEVICES)

~28 BITS OF ENTROPY

$2^{28} = 3$ DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE PHRASES ON A NEW DEVICE ARE SOMEWHAT COMMONER IN THEIR MINDS AS PHRASES, BUT AS NOT WHAT THE MINDS WERE DEVELOPED FOR)

DIFFICULTY TO GUESS: EASY

DIFFICULTY TO REMEMBER: HARD

WAS IT TROUBADOR? NO, TROUBADOR, AND ONE OF THE 0s WAS A ZERO? AND THERE WAS SOME SYMBOL...

THAT'S A BATTERY STAPLE. CORRECT!

~44 BITS OF ENTROPY

$2^{44} = 530$ YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS: HARD

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<http://xkcd.com/936/>

Keeping Your Passwords Safe

- Never use the same password on more than one account.
- Write down your passwords in a notebook and put it somewhere safe and memorable.
- Don't save your passwords in a Word file on your computer.
- Consider not letting your Web browser save your passwords.

Password Managers

Apps that will automatically generate strong passwords for you and input them whenever you need to log in to a website.

If you use one:

- Create an extra-strong master password
- Use 2-factor authentication

Password Managers

- LastPass (free and paid versions) (www.lastpass.com)
- Dashlane (free and paid versions) (www.dashlane.com)
- Keeper (free and paid versions) (www.keepersecurity.com)
- 1Password (paid only) (1password.com)
- Windows Hello (Windows 11) – PIN, fingerprint, FaceID

Safety Tips


Tips for Safe Internet Use

- Only download from official company websites (watch out for misspellings).
- Do not click on pop-ups, strange links, or ads.
- Force quit pop-ups using Task Manager (CTRL+ALT+DEL) on Windows or Command+Option+Esc on Mac.
- Do not give out personal information to a site you don't trust.
- If it sounds too good to be true, it probably is.

Secure Connections

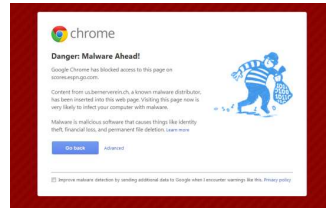
Only send sensitive information (such as a credit card number) over a secure connection.

Two ways to tell if a connection is secure:

- The URL starts with **https://**
- There is a **lock**  icon displayed somewhere in your browser window.

Browser Warnings

- Your Internet browser may warn you if you are visiting a site that is not secure, or has an expired security certificate.



Browser Warnings

- In general, avoid sites that have one of these warnings.
- On rare occasions, a good website may be blocked by your browser.
 - ✓ If you have visited the site previously without issue, they may have simply forgotten to renew the certificate.
 - ✓ Or your browser may be out of date.


Google Transparency Report

You can use Google Transparency Report (<https://transparencyreport.google.com/safe-browsing/search/>) to check the trustworthiness of websites – click on Site Search.


Buying Online

To limit vulnerability when purchasing, consider a secure payment method.

Examples:

 PayPal (www.paypal.com)

 Apple Pay (www.apple.com/apple-pay/)

 Google Pay (www.pay.google.com)

Tips for Safe Email Use

- Only download attachments/click on links if the email is from an address you trust.
- Check the email address, not just the name.
- If your friend's email doesn't sound like your friend, they were most likely hacked.
- Do not respond to requests for personal information (unless it's someone you already know who has a legitimate need.)

Tips for Safe Email Use

- Never give out usernames or passwords over email.
- Be cautious about clicking on links. Consider using a search engine to find the page instead.
- Copy and paste text from suspicious emails into a search engine to see if it is a known scam.
- Sign up for Scam Alerts from the FTC to stay informed about currently popular scams.
(<https://www.consumer.ftc.gov/features/scam-alerts>)

2-Step Verification

- Requires you to enter not only your username and password, but also a one-time code that's texted to your phone.
- Keeps attackers from accessing your account by figuring out your password.
- Notifies you right away if someone is trying to access your account.

Spam

- Mark unsolicited, unwanted email as spam in your email program.
- Set up custom filters to send email to the spam folder automatically based on senders or keywords.

Updating

- Keep all software on your computer, especially your operating system, up-to-date.
- Avoid using operating systems that are no longer supported.
 - ✓ Support for Windows 8.1 ends in January 2023.
 - ✓ Windows 10 supports lasts until 2025.

Backup

Make copies of your computer's files so they can be restored if lost.

- Local backup - back up to a flash drive or external hard drive.
- Online backup - back up your data automatically to the cloud. Popular services include
 - ✓ iDrive (www.idrive.com)
 - ✓ Carbonite (www.carbonite.com)

VPNs

- Used to encrypt the information you are sending over the Internet
- Disguise your computer's IP address so your traffic cannot be easily tracked to you.
- or consider subscription services like TunnelBear (www.tunnelbear.com) and ExpressVPN (www.expressvpn.com).

Private Search Engines

- Do not sell or track your personal information.
- Do not allow ads to target you.

Examples:

- ✓ DuckDuckGo (duckduckgo.com/)
- ✓ StartPage (www.startpage.com/en/)

Data Breaches and Digital Shredding

- Have I Been Pwned (haveibeenpwned.com/): see if your email was part of a data breach
- Create a Google Search Alert (www.google.com/alerts)
- Privacy Fix: How to Find Old Online Accounts (<https://www.consumerreports.org/digital-security/how-to-find-old-online-accounts-a1266305698/>)

Mobile Device Security

- Always keep your operating system up to date.
- Protect your device with a passcode.
- Back up important data regularly.
- Only download apps from an official app store.
- Be wary of apps requesting unnecessary permissions.
- Install antivirus software.
- Be careful on public Wi-Fi networks, particularly if unsecured.