MALWARE

FOR MORE INFORMATION:
SECURITYEDUCATIONCOMPANION.ORG

MALWARE, short for malicious software, is any program that's designed to conduct unwanted actions on your device.
Examples of malware include:

- computer viruses
- programs that steal passwords
- programs that secretly record you
- programs that secretly delete your data

MALWARE THROUGH PHISHING

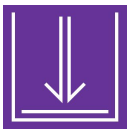
Phishing is when an attacker sends a message, email, or link that looks innocent, but is actually malicious. Phishing often involves impersonating someone you know or impersonating a platform that you trust.

Note: Not all phishing includes malware. Sometimes an attacker wants to steal passwords to a service and might do so by impersonating a website, without installing malware on the user's device.

COMMON WAYS MALWARE IS INSTALLED

OPENING A MALICIOUS ATTACHMENT OR FILE
A malicious attachment is often shared in phishing messages.

CLICKING A MALICIOUS LINK
A malicious link is often shared in phishing messages.



DOWNLOADING UNLICENSED SOFTWARE
Software that cannot receive security updates increases risk (e.g. not from the Apple App store or Google Play store.)

VISITING COMPROMISED WEBSITES
Sometimes websites are taken over and are used to host malicious content.

DOWNLOADING AUTOMATIC CONTENT
Attackers may gain access to a network and can use this network to spread malware.

SHARING USB DEVICES OR PLUGGING INTO SUSPICIOUS PORTS
A charging station or port can be used to download malware.

TYPES OF MALWARE

ADWARE
ads everywhere

This malicious software usually attempts to display advertising to the user via overloading pop-ups or other methods. Some adware tracks information on the user or extracts personal information. Adware, like other malware, can be bundled with other software, often downloaded from non-reputable sources, such as outside of official app stores or from the software developer..

STALKERWARE
when your device helps your stalker

Stalkerware runs silently and gives the attacker full control over a device. Stalkerware can be installed when somebody has physical access to your device (such as a family member or partner, "let me use your phone for a moment") and installs a stalkerware app or when a user gets tricked into downloading the app.

TROJAN
like a gift but an attack in disguise

When downloaded, Trojan software may perform like the intended legitimate application, but is in fact doing malicious things in the background. This is often found in pirated or "cracked" software or fake antivirus software.

RANSOMWARE
software holding you hostage

When downloaded, this malicious software holds a company, organization, or individual's data for ransom. Ransomware gained popularity in the last decade and is now a multi-million dollar business for attackers around the world.

A.P.T. ATTACK
Advanced Persistent Threat

An A.P.T. attack is malware from an adversary with sophisticated capabilities and substantially more resources dedicated to achieving their goals: compromising your system. A.P.T. attacks are often used simultaneously with nation-state actors who will attempt to maintain "persistence," or long -term access, to the system they are targeting.

PROTECTION

FOR MORE INFORMATION:
SECURITYEDUCATIONCOMPANION.ORG

5 TIPS FOR DEFENSE AGAINST MALWARE

TIP #1: UPDATE YOUR SOFTWARE (& CHECK YOU ARE USING LICENSED SOFTWARE)*

Most malware take advantage of known vulnerabilities. The software companies themselves often fix these vulnerabilities and push to users through **updates**.

Software updates are therefore critical for user security, as they are the most sure way to stay up to date on fixing known vulnerabilities that attackers might use.

***If you're not sure how to get licensed software, ask your friendly digital security facilitator for tips and available resources.**

TIP #2: BACKUPS FOR THE FUTURE

Back up your data today and future-you will be grateful. If you lose your device (whether to malware, theft, or the device just not turning on) all is not lost: your files will be in your backups. Protect those backups by using a strong password and encryption.

TIP #3: PAUSE BEFORE YOU CLICK

Link and file sharing is a common practice, but stay vigilant when interacting with or sharing links. Before clicking, ask: does this feel strange?

LOOK OUT FOR...

- ***SHORTENED & CUT-OFF LINKS***
  - Links and emails may preview as shorter when viewed on a phone than when viewed on a computer. Link shorteners like bit.ly & similar services can redirect to malicious sites.

    Tip: Try a service like **https://unshorten.it** to see the full expanded URL!

- ***IMITATION, THE GREATEST FORM OF TRICKERY***
  - Typos, similar characters, and copied branding are out to trick you. Verify that it's the actual service.

    Tip: When you're on an authentic service, use a **bookmark**: this can make it easier for your computer to help you remember legitimate websites addresses.

    Tip: Save the correct link in your password manager: a **password manager** can remember designated sites and fill in your password for you.

  - Beware of "social engineering," like receiving a message from someone pretending to be your friend.

    Tip: Reach out to your friend over another form of communication and verify it's really them.

- ***ACCIDENTAL TAP OR CLICK***
  - When examining links on your device, one tap or click might accidentally open the link!

    Tip**:** If using a mouse, take advantage of **hovering** to see the full link.

TIP #4: BE WARY OF PHYSICAL ACCESS

Sometimes, our adversaries are people we know, or people who can access our devices when we aren't paying attention. Using full-disk encryption and a strong password to protect your device can help defend it from unwanted physical access. Use caution when lending your unlocked device to someone. To read more, check out **ssd.eff.org**.

TIP #5: USE AN ANTIVIRUS

Not all antivirus is created equal; some software marketed as antivirus can be disguised malware. You may want to use your device manufacturer's own antivirus. If you prefer third-party antivirus software, check for:

- independent reviews of the software
- if the antivirus website has **an up-to-date list of malware*** on the type of malware and adversary you are concerned about

***Published threat research can indicate the antivirus has an active team defending against this type of malware.**

I THINK I HAVE MALWARE. WHAT SHOULD I DO?

Is something strange happening on your device? Is it a specific account that has been affected (like social media), or is it the whole device? If it seems like malware, be careful of how you use and carry that infected device in the future—then, use a **different device*** to contact a specialist for help.

***A separate device would be unconnected to the malware-affected device. This could be a library computer or a trusted friend's phone, for example.**

CONTACT A TRUSTED TECHNICIAN

Keep a **log**, like the strange messages you received in their original form (e.g., if it's an email, forward the original email with header metadata, not a screenshot). Include details: **date, time,** and **description.** Send these to a trusted technician.

ASSESS THE DAMAGE

What sensitive information may have been compromised? Should you change any of your passwords or accounts? Plan next steps for safety by doing a risk assessment (aka "threat modeling").

FURTHER READING

SECURITYEDUCATIONCOMPANION.ORG > SECURITY EDUCATION 101
Software updates and why they're important

SSD.EFF.ORG:
How do I protect myself against malware
How to avoid phishing attacks