STONEBROOK
PRIVATE

What to do in the case of a typical hacking or phishing attack

The Most Common Cybersecurity Attacks

Phishing: This is when hackers send you an email or a message that looks like it comes from a legitimate source, such as your bank, your employer, or a popular website. The message usually asks you to click on a link, enter your personal information, or download an attachment. The goal is to trick you into giving up your login credentials, your financial data, or your identity.

Ransomware: This is when hackers infect your device with malicious software that encrypts your files and demands a ransom to restore them. Ransomware can lock you out of your important documents, photos, videos, or other data. The hackers may threaten to delete your files or expose them to the public if you don't pay.

Spyware: This is when hackers install a program on your device that secretly monitors your online activity, keystrokes, passwords, or webcam. Spyware can steal your personal information, your browsing habits, your contacts, or your location. Spyware can also slow down your device, drain your battery, or display unwanted ads.

You clicked on a Phishing/Scam/Spyware email link, now what?

- Clicked the email link but didn't enter information or download anything.
    - You should close the browser window immediately and delete the email from your inbox. You should also run a virus scan on your device to make sure it is not infected with malware.
- Clicked a link in the email and provided personal details like username or password.
    - Change your passwords for all online accounts immediately, monitor bank statements and credit reports for unauthorized activity, and alert your bank and any relevant institutions about the phishing attempt to prevent or reverse fraud.
- Clicked a link in the email and downloaded an attachment.
    - You should disconnect your device from the internet and turn it off. You should also contact a trusted IT professional or service provider to help you remove the malware from your device and restore your files. You should also follow the steps above for changing your passwords and checking your accounts.

Your machine is encrypted and you received a ransomware demand?

- Disconnect your device from the internet and any other networks or devices it may be connected to. This will prevent the ransomware from spreading to other devices or encrypting more files.
- Do not pay the ransom or contact the attackers. Paying the ransom does not guarantee that you will get your files back, and it may encourage more attacks in the future. Contacting the attackers may also expose you to further risks or scams.

- Report the incident to an IT professional, or service, your security/antivirus provider, or law enforcement agency. They may be able to help you recover your files, identify the source of the attack, or prevent further damage.

Tools to Keep You Safe

Malwarebytes: Renowned for its effectiveness in detecting and removing malware, including viruses, trojans, and spyware. It's user-friendly and offers both free and paid versions.

Norton 360: Offers comprehensive protection including virus removal, firewall, and even VPN services for online privacy. Norton is a well-established name in cybersecurity.

Kaspersky Internet Security: Known for its robust malware detection capabilities. It provides a range of features including virus removal, system scanning, and internet security.

Bitdefender Antivirus: Offers powerful malware and ransomware protection. It's highly rated for its advanced threat defense and minimal impact on system performance.

Quick Scan Approach

If you think you may have malware or potentially have downloaded an infected file or clicked a bad link. The Malwarebytes tool is a good way to quickly download and test your system for free. Below is that process.
NOTE: Be sure to uninstall after you do this to avoid the nagging pop-ups and alerts to sign up for the service.

1. Go to the Malwarebytes site and download the free version of Malwarebytes (www.malwarebytes.com)
2. Install the application – be sure to always select the "Free" option. It may prompt multiple times to sign up for their service. You can bypass this and install completely free.
3. At the end of the installation the software can be run and do a full scan of your system.
   a. If items are found, you have the option of cleaning them out or having the system delete the files, but also remember to follow the guidance in the sections above as well.
4. Once you have completed the scan, do a complete uninstall of the Malwarebytes tool. Click here for uninstall instructions if you need help.