THE ANDOVER COMPANIES

PREVENTION AND SAFETY TIPS TO HELP YOU

RECOGNIZE AND STOP A HOME CYBERATTACK

It is hard to remember a time when computers, cell phones, smart appliances, virtual assistants, and other similar devices were not helping us navigate life. Although useful, all this connectivity does leave you more vulnerable to cybercriminals looking to hack into your home network, place malicious spyware on your devices, hold your personal data hostage, and worse.

7 COMMON HOME CYBERTHREATS

If a home cyberattack is successful, it can lead to devastating financial losses, stolen identities, and disrupted lives. Making sure everyone in your household knows the main cyberthreats and how they work may help block them.

#1 Malware:
Malicious software, like viruses or spyware, that bad actors secretly install on computers, tablets, phones, and other digital devices, usually to steal sensitive information.

#2 Spoofing:
Online scammers disguise their identity, via a faked email or text address, website URL, or caller ID number, as someone you know and trust, like a friend, coworker, or business, to spread malware, steal money or data, or gain access to your devices.

#3 Phishing:
Typically starts with an email trying to trick you into clicking on a fraudulent link or attachment that often brings you to a form asking for sensitive information like usernames; passwords; and Social Security, credit card, or bank account numbers.

#4 Smishing:
Similar to phishing, but usually starts with an "urgent request" text message containing a sham link that, if clicked, may take you to a form used to steal your information or download malware onto your device.

#5 Vishing:
Calls or voicemails in which a scammer pretends to be a legitimate company and attempts to get you to give out personal information or to record your voice so they can use it to authorize charges or access financial accounts.

#6 Ransomware & Cyber Extortion:
Two cybercrimes that hijack your devices with the aim of extorting money, but in different ways. Ransomware encrypts your data and programs, while cyber extortion steals your personal information.

#7 IoT (Internet of Things) Attacks:
Hackers take over smart home devices, like door locks, speakers, lightbulbs, appliances, toilets, robot vacuums, and even toys, causing mayhem.

Did You Know?

- At any given time, 4.1 million websites are infected with malware.
- The number of ransomware attack victims rose by 128% from 2022 to 2023.
- More than 350 million people were impacted by personal data breaches in 2023.
- 74% of account takeover attacks start with phishing.

10 STEPS YOU CAN TAKE TO MINIMIZE THE RISK OF A HOME CYBERATTACK

This checklist offers several simple and effective ways to help you safeguard your home and family from today's cyberthreats:

FORTIFY YOUR HOME WI-FI NETWORK.

Use strong, unique passwords; enable encryption protocols; and consider setting up a separate guest network to prevent unauthorized access.

IMPROVE YOUR PASSWORD PROTECTION.

Change default passwords on all devices to unique, complex ones with a combination of letters, numbers, and special characters.

ADD EXTRA LAYERS OF AUTHENTICATION.

Enable multifactor authentication for logging in to all devices and online accounts.

REGULARLY UPDATE SOFTWARE.

Check for device software updates and install them right away, either manually or via auto updates if available.

RUN DATA BACKUPS.

Back up the data on all devices to an external storage drive or to the cloud so everything from photos to financials can be recovered more easily if compromised.

BE SKEPTICAL OF LINKS, ATTACHMENTS, AND MESSAGES.

If unsure whether an email or text is from someone you know and trust, use another contact method you are confident in to get verification.

KEEP PERSONAL INFORMATION PRIVATE.

Put documents like Social Security cards and bank statements in a secure, fireproof place, and shred them before you throw them away.

SHARE CAUTIOUSLY ON SOCIAL MEDIA.

Before posting information about yourself or your family, consider whether a bad actor could use it to identify you, manipulate you, or guess an account recovery question.

CONFIRM A WEBSITE IS SECURE.

Look for critical signs before you make a transaction, including a lock symbol by the URL address, "https" in the URL, and a PCI DSS compliance certificate.

REPORT YOUR SUSPICIONS.

Help make your community (online and offline) safer by notifying local authorities and the FBI's Internet Crime Complaint Center (IC3) of potential online fraud.

Sources:

Identity Theft Resource Center 2023 Annual Data Breach Report

Egress 2024 Email Security Risk Report

Security Affairs 2023 Ransomware Attacks Report

SiteLock 2022 Website Security Report

https://consumer.ftc.gov

https://www.experian.com/blogs/ask-experian/phishing-smishing-vishing/