Cyber Attack

You don't have to be an IT guru to understand the real threat that comes from cyber-attacks. Cyber-attacks are any malicious Internet event meant to invade privacy of the user or network. Attacks might be destructive and do great harm to a single user's device or the network on which the device operates. But some attacks will not be detected by the end user.

Whether you are working with a company on a network or independently (privately) everyone online is vulnerable and everyone is potentially a target. This activity will help you recognize common types of attacks and ways to avoid or prevent them.

End-User Attacks

Malware

Includes viruses and ransomware running on your device. Malware can take over the operation of your device or quietly watch your operations and keystrokes and steal confidential information from your network. Malware usually requires the user to initiate by unwittingly installing the malicious software.

Phishing

Pretending to be someone you trust or a system you work with, to get you to visit a fictitious site and enter your login or other private info.

Trojan Horse

Malware disguised as a trusted source that convinces the user to open a link or an attachment and install itself.

Virus

Malware that spreads by users from an infected device to the rest of the devices on a network/system.

Worm

A type of virus that does not rely on users to copy and spread but can replicate itself, once inside a network/system.

Spam

The unethical distribution of mass digital messages. This is the main way that malware is opened and spread.

Rootkit

Malware that accesses or controls a device without being detected.

Server Side Attacks

Unless you work on the server end of things (Network Administration) you probably won't encounter the following, but it is still helpful to be aware of them.

Credential Reuse

If hackers are able to target vulnerabilities on any site you use to login, they often apply that same login information to other major sites to see if you reused your login and password.

SQL Injection Attack

Structured query language (SQL) is a programming language used to communicate with databases. The injection attack targets the server side to get customer information from the database, such as credit card numbers. This is not an end-user attack, but communicates directly with the server.

Warning signs that you might be infected

- Your friends tell you that they are receiving emails in your name, but you are not sending them.
- Your device is grinding, overworked, CPU levels are high, crashes
- Browser load times are slow, programs/apps stall
- Connectivity problems
- Odd device behavior, mysterious files/icons appear
- OS warnings are triggered

Best Practices for Secure Browsing

Here's an article from Nate Lord at Veracode, "Best Practices for Secure Browsing: Cybersecurity 101" which I have summarized below. Please go to the article to read more.

- Keep your browser software up-to-date.
- Keep your anti-virus software up-do-date and on a daily scan schedule (note: some employers do this for you, but check to make sure).
- Watch out for phishing.
- Don't reuse passwords.
- Use HTTPS.
- Read privacy policies.
- Regularly monitor your bank statements.
- Avoid public or free Wi-Fi.
- Disable stored passwords.
- Turn on your browser's popup blocker.
- Become familiar with your organization's Internet Use Policy, if one is available.


CTECS
WRS
WORKPLACE READINESS SKILLS
Assessment


CTECS
Career and Technical Education
Consortium of States

Cyber Security Awareness Activity

Read the following scenario and link the issue to one or more of the terms referenced in this document.

1. You receive an email that appears to be from your work network, marked urgent, with the subject line “Fraudulent activity has been detected on your account.” To find out more, you click and follow the link that is supposed to contain more information about how you can stop the fraud. You go to what appears to be a trusted site which asks you to log in.

   What type of attack is this? How can you prevent it?

2. When my banking site got hacked two years ago but the security problem was resolved without a problem. However, my credit card account was just hacked and a thief made purchases with my account number.

   What happened?

3. Suddenly your device begins operating on its own and you have lost control.

   What is responsible for this?

4. Your company’s server has suddenly been hacked by fake code and your customer database has been copied by an unknown source, including login information.

   What type of attack is this? How can it be prevented?

5. Web surfing suddenly takes a much longer time than it once did.

   What could be the issue? What is a good solution?