Protecting Yourself Against Cyber Attacks

Cyber attacks can have devastating consequences for your systems, data, and business. Understanding the risks and knowing the steps you can take in the event of an attack is paramount to keeping your data safe and your business running.

Understanding the Risks

Cyber criminals are opportunistic. At any given time, they use any vulnerability to outsmart their victims. During the COVID-19 pandemic, you need to be acutely aware of emails that appear to be from trusted organizations such as the World Health Organization (WHO) or the U.S. Center for Disease Control (CDC).

Cyber criminals send official-looking information under organizations' names that contain phishing schemes that attempt to trick the recipient into opening attachments or clicking on links that can release damaging malware, ransomware and more.

Companies or organizations with many remote workers can be particularly at risk. Remote workers who aren't working under tight cybersecurity measures are vulnerable as they may not have the built-in tools to flag potential attacks.

Many Forms of Attack

Phishing is a fraudulent attempt to fool someone into revealing their pins, social security number, credit card or bank account information. They then use this information to steal funds from bank accounts or use credit cards to make purchases.

Malware is software that gains access to and damages a computer system. A malware attack happens when that software infiltrates the system and performs activities, such as code changes, without the user's knowledge. Malware can be activated by opening unknown email attachments, downloading from nonsecure sites, etc. Once unleashed, it can spread throughout an entire network.

Ransomware is a form of malware that damages, freezes or encrypts computer files until a ransom is paid. Even if the ransom is paid, the cybercriminals may refuse to unlock the system or publish information they have stolen from the system until more payments are made. A ransomware attack can make data corrupt or unavailable to the user and can be combined with a data breach.

Preventing Cyber Attacks

- Update software and operating systems patches regularly or as soon as the patches become available.
- Segment older or unused applications as they are most susceptible to attacks.
- Never click on unknown or questionable links or attachments.
- Regularly back-up data. Store back-ups in a separate place.
- Restrict or forbid users from downloading software. Give access to applications only if needed.
- Use spam filters to flag suspicious emails.
- Train your staff on the potential threats. Run periodic phishing tests that appear to be real phishing scams.
- Keep software up to date.
- Don't use mobile devices for sensitive information.

Responding to an Infection

- Turn off the computer or device.
- Isolate the computer or device from any network, Bluetooth, or wireless connection.
- Notify the appropriate internal authority—IT security, a supervisor or business owner right away.
- Put backup data offline to secure it.
- Change all passwords.

HSB
A Munich Re company

HSB
One State Street
P.O. Box 5024
Hartford, CT 06102-5024
Tel: (800) 472-1866

hsb.com