elevITy®

CYBERSECURITY Tips for Employees

Hackers are targeting your organization to gain access to sensitive information or hold critical data hostage by installing malware. Protect yourself and your company from the growing risk of cyberattacks with these tips.

INTERNAL THREATS

Not all cyber criminals gain access from outside your organization. Safeguard your data from the inside out with these best practices:

- Lock your computer screen while away from your desk
- Place sensitive documents in locked cabinets
- Never write usernames or passwords on paper
- Keep flash drives, mobile devices and keys secure
- Require a PIN or badge/card reader to authenticate and release printer documents

Just the Facts. Think Before You Link!

That Click May Have Consequences.

- **60%** of small companies **go out of business** within 6 months of a cyberattack
- It costs the average small business **$690,000 to recover** from a cyberattack
- **62%** of all cyberattacks **target small and mid-sized businesses** - about 4,000 every day

PASSWORDS

Don't make a cyber criminal's job any easier. Create strong passwords that help keep information secure.

- Avoid using common and easy-to-guess passwords such as "**password**" or "**123456**"
- Do not use personal information such as birth or anniversary date
- Add complexities such as random capital letters, symbols or numbers (e.g., **L!keTh1$**)
- Create separate passwords for each account
- Change passwords every 90 days

EMAIL

Email phishing schemes are the #1 access point for cyberattacks. Many admit to knowing the threat, yet click on suspicious links anyway.
Instead, follow these steps:

- Never forward suspicious emails
- Confirm the sender's identity - when in doubt, call or send a separate email
- Check for spelling errors in the email's body, address or domain URL
- Don't click on attachments you weren't expecting to receive
- Contact IT if there's any hint of suspicious activity
- Never reveal confidential information such as account numbers, passwords, etc.

PERSONAL DEVICES

Many employees use company-issued or personal devices for work email and other functions. Ensure that sensitive data doesn't get into the wrongs hands by taking these precautions:

- Make sure your device is **password protected**
- Avoid using **public Wi-Fi**, it's likely **not secure**
- Install any recommended **security patches** or **updates**
- Install a **"wipe" function**. If the device is lost or stolen, data can be erased remotely
- Install **anti-virus software**
- **Don't install obscure apps** or software from disreputable providers

When in doubt, contact your IT department to investigate any suspicious activity, or reach out to the experts at Elevity to speak with one of our vCIOs.

888.733.4060 | elevityIT.com