Cybersecurity Tips for Work and Home

Cybersecurity breaches are all over the news lately, and incidents seem to be multiplying by the day. Do you know how to defend yourself and your organization against them? Implement these easy strategies to keep yourself and your company from getting hacked, embezzled, or ransomed.

BUILDINGS®

UNDERSTAND THE THREAT

Bad actors use these three strategies to gain access to valuable data belonging to people or organizations.

Ransomware: Malicious software that encrypts the data on your computer or another device. This data could contain emails, databases, or other important information. You must then pay a ransom, often in the form of untraceable Bitcoin, to get your information back.

Social engineering: When bad actors use deception to manipulate someone into divulging personal information, which can then be used for fraudulent purposes. Phishing is a type of social engineering in which someone sends an email or another type of message that appears to be from a reputable company to gain passwords, credit card information, etc.

Brute force hacking: Using techniques to gain access to a network.

REDUCE YOUR RISK TODAY

Implement these strategies to improve your security posture at home and work.

- **Passwords and PINs:** Use passwords, PIN codes, and touch ID wherever possible. Don't assume you have nothing to hide. Make sure no one can get easy access to your passwords and PINs, and don't reuse passwords or codes.
- **Password management:** Use a password manager that generates new, secure passwords for you and keeps them in a vault. Password managers are available for computers, phones, tablets, and more. This is much more secure than saving passwords in your browser.
- **Authentication:** Implement two-factor authentication (2FA) or multi-factor authentication (MFA) wherever you can, from your email accounts to social media. This six-digit code helps keep your systems safe.
- **Encryption:** Make sure your devices are encrypted. This ensures that no one can access data from your device even if they gain access to the device itself. Backups should also be encrypted.
- **Browsing:** When you browse the internet, look for the lock icon in the browser that indicates a secure socket layer (SSL).
- **Backups:** Use backup software. Both iOS and Android have built-in backup software. For your computer, invest in a secure cloud-based backup option like Backblaze or CrashPlan and combine that with local backups on external hard drives that you test regularly. Your IT department should already be doing this with your professional data, but you'll want to do the same with your personal files.
- **Permissions:** Watch permissions when you install new apps. Make sure you're not granting access to parts of your phone that apps shouldn't have access to—for example, Candy Crush doesn't need access to your contacts. Whenever you download software to your computer, ensure that you're on the authentic manufacturer website—it won't always be the first search result, so review carefully.
- **Updates:** Stay current with updates. Install any patches issued for your hardware or software. Don't let your systems run without being patched. These updates can close important security gaps.
- **Email security:** Never use your personal email for business purposes. Use scam filtering software for your personal email (your IT department is probably already taking care of this for your professional email). Don't open PDFs whose source you don't recognize. If you receive an invoice, hover over the master link and see if it matches the sender—for example, a UPS email should be coming from UPS.com, nowhere else.