Cyber Security and Safety Tips

By: Mike Smith host of Mike Tech Show podcast, Sept 2024

miketechshow.com

1. **Be alert**: Use common sense and think twice before clicking links, opening attachments, visiting websites or responding to emails or phone calls. Many cyberattacks can be prevented if you take a moment to consider your actions and potential consequences.
2. **Know how to identify phishing attempts:** Be wary of emails or calls that require "immediate action" or ask for personal information. Carefully inspect links to make sure they point to a reputable site before clicking and never respond to messages asking for your username and password.
3. **Use 2FA:** Use 2-factor authentication (2FA) for accessing any services or email on the web. Examples: Facebook, banking, credit cards, Amazon. Whenever it is available enable 2FA. This extra layer of security requires you to verify your identity twice before accessing your account and can protect you from having your email hijacked or paycheck redirected.
4. **Create strong passwords:** Make a lengthy password using a combination of uppercase and lowercase letters, numbers and special characters. Use different passwords for different sites and consider using a password manager, such as RoboForm, to store your passwords. Also, never share your password with anyone.
5. **Security question answers:** When you reply to specific security questions, spell your answer backwards or add a pin number before and/or after you answer.
6. **Lock your devices:** Never leave your devices unattended. Password protect your phone or tablet and log off or lock your screen every time you step away from your computer. (Win+L)
7. **Keep apps and software up to date:** Talk with your IT support staff to make sure your work computer is programmed to automatically install updates. Do the same thing for your home computer and mobile devices, and regularly restart all devices to give them a chance to complete the update process.
8. **Limit activities on public Wi-Fi:** When traveling, either use your cellular network, or a virtual private network (VPN) to get secure internet access. If you must use a public network, make sure it is reputable and refrain from accessing sensitive information, such as online banking.
9. **Back up your computer:** Talk with the IT support staff and make sure there is a plan in place to back up your files and data regularly. Regular backup will protect you from losing all your work in the event of a ransomware attack.
10. **Protect personal information:** Do not store personally identifiable information—such as Social Security number, credit card numbers on your computer unless it's in an encrypted file.
11. **Screen all phone calls:** Set your home phone to the lowest number of rings and let calls go to voicemail. Only answer or return calls to people you know. If you do answer, do not be afraid to hang up. Never give personal information over the phone.
12. **Do not reply to unknow text messages:** Be skeptical of text messages, especially those that request personal information or urge immediate action.
13. **Do not call:** If any number pops up on your computer screen that asks you to call, don't do it. Do not allow a stranger to remotely access your computer.
14. **Type the exact website address (URL):** Do not search for a company's support phone number. Go to their exact website to find the proper number. Sometimes the top search engine results are ads and not a direct link to the real company.
15. **Freeze Your Credit:** Sign up for a Security Freeze at all three of the credit bureaus. (Experian, Equifax, and TransUnion)