CYBERSECURITY BEST PRACTICES

Not sure where to start with cybersecurity? Here's a top ten list of cybersecurity tips that could help protect you from cyber threats.

1. You're A Target

Don't ever say "It won't happen to me." You're an attractive target to hackers.

2. Good Password Management Is Important

Be sure to use unique, secure passwords, which should include at least eight characters with a combination of upper and lower case letters, numbers and special characters. Don't share your passwords with others and don't write passwords on a sticky note and place them under your mouse pad. To help keep track of your unique, secure passwords, consider a password management platform such as LastPass or 1Password.

3. Never Leave Your Devices Unattended

If you need to leave your computer, phone or tablet unattended for any amount of time, be sure to lock it so no one can use your device while you're gone. If you keep sensitive information on a flash drive or external hard drive, be sure to lock it up as well. Work with your IT department to automatically lock screens on your company's devices or workstations after they have been idle for a few minutes.

4. Connect Securely

Don't connect to a public or unsecure WiFi to do any confidential work or sensitive browsing such as banking or shopping. Whether it's a friend's phone, a computer in a hotel's business center or a cafe's free WiFi – your data could be copied or stolen. When using WiFi, be sure to use a network you trust. Utilizing a VPN or other secure connection provided by your company's IT department are great options.

5. Back Up Your Data

It's important to back up your data regularly and to make sure your anti-virus software is up to date. If your backup data leaves the office, be sure the data is encrypted.

6. Know What You're Plugging Into Your Computer

Malware can be spread through infected flash drives, external hard drives and even smartphones, so be conscientious of what you're plugging into your computer.

7. Watch What You're Sharing On Social Media

Hackers can befriend you and easily gain access to lots of information about your personal life that could help them gain access to more valuable data. Be sure to monitor your accounts for any suspicious activity. If you see something unfamiliar, it could be a sign you've been compromised. Be sure to have a social media policy in place for your employees.

8. Keep Your Operating Systems Updated

If you're running Microsoft Windows or Apple OS X, set your operating system to receive automatic updates. System updates are important for server operating systems where patches can be reviewed and updated on a recurring schedule.

9. Protect Mobile Devices

If a company laptop or mobile phone is misplaced or stolen, have a process in place that notifies your IT department and erases the device's company data remotely.

10. Update Your Policies

Review your IT policies and provide reminder training to employees at least annually for new and updated policies. Be sure to look beyond the traditional policies and include policies for new topics such as bringing your own devices from home or remote access.

BOK FINANCIAL

Sources: Top Ten: The Most Important Cyber Security Tips For Your Users: https://umbrella.cisco.com/blog/2013/10/08/top-ten-important-cyber-security-tips-users/. Top 20 Items That Must Be On Your Cybersecurity Checklist: https://www.symtec.com/top-20-cybersecurity-checklist/.

GE-RE-D86