Cyber Safety

Protect yourself and your personal information

10 KEY CYBER SAFETY TIPS

1. Never click on a link in an email until you validate the source
2. Never enter personal information in an email or text message
3. Use antivirus software and keep it up to date
4. Limit web usage in the office to core, business-related sites
5. Make minimal use of unsecured, public networks
6. Create strong passwords and change them every 2–3 months
7. Do not use the same password for multiple accounts
8. Create separate email accounts for work, personal use, alert notifications and other interests
9. At home, set up a primary network and another for guests
10. Be prudent in what you share about yourself and your job via social media

Put these safeguards in place as soon as possible—if you haven't already.

passwords

- ☑ Create passwords that are at least 10–14 characters; use a mix of numbers, upper- and lowercase letters and symbols
- ☑ Change passwords three to four times a year
- ☑ Store in a safe place or utilize a password management tool
- ☒ Do not use the same password for multiple accounts
- ☒ Do not create common passwords
- ☒ Do not select "remember my password" on websites you visit

email

- ☑ Create separate email accounts for work, personal use, alert notifications and other interests
- ☑ Turn on two-factor authentication whenever an ecommerce site offers it
- ☑ Encrypt important files before emailing them
- ☑ Use spam filtering to stop unwanted email from reaching your in-box
- ☒ Do not open emails from unknown senders
- ☒ Do not reply to requests for financial/personal info

virus and malware protection

- ☑ Keep software/browser/systems up to date
- ☑ Install antivirus software and keep it up to date
- ☑ Turn on firewall to highest level
- ☑ Regularly back up your data
- ☒ Do not install or use pirated software
- ☒ Do not install P2P file-sharing programs
- ☒ Do not set email to auto-open attachments

internet usage

- ☑ Download software only from trusted sources
- ☑ Log out of sites instead of simply closing the window
- ☑ Look for https:// for secure session validation
- ☒ Do not click on links from unknown/untrustworthy sources
- ☒ Do not allow ecommerce sites to store your credit card information
- ☒ Do not click on pop-up windows to close them; instead use the "X" in the upper right hand corner of the screen

mobile

- ☑ Keep screen lock on; choose strong passwords
- ☑ Select a device with anti-theft features
- ☑ Turn off Bluetooth when it's not needed
- ☑ Regularly update apps (e.g., security patches)
- ☑ Securely back up your data
- ☒ Do not click on ads when surfing the internet

public Wi-Fi/hot spots

- ☑ Disable ad hoc networking
- ☑ Turn off auto connect to non-preferred networks
- ☑ Turn off file sharing
- ☑ Consider using your phone's mobile network instead
- ☒ Do not use/avoid public Wi-Fi
- ☒ Do not use public Wi-Fi to enter personal credentials; your keystrokes can be captured by hackers

home networks

- ☑ Create one network for you, another for guests
- ☑ Change your router's name and password
- ☑ Change the password to your wireless network
- ☑ Turn on your router's WPA2 encryption and firewall
- ☒ Do not use default user names/passwords
- ☒ Do not broadcast your home network

social engineering

- ☑ Telephone the person who sent the email to confirm its authenticity if you suspect it may be fraudulent
- ☑ Limit the amount of personal information you give out
- ☑ Use privacy settings online wherever possible
- ☒ Do not respond to requests for personal or financial information in an email
- ☒ Do not open an attachment from someone you know if you are not expecting it; call to confirm before clicking
- ☒ Do not assume that every email you receive is authentic

Cyber Safety

Choosing services, software and equipment

email providers

Email is one of the most essential online services used today. If your email is compromised, your personal information (accounts, communications, phone numbers, addresses, etc.) can be stolen. The best email providers surround your information with several layers of security.

FEATURES TO LOOK FOR

Authentication

A high-quality email service will provide secure authentication to prevent spam and spoofing.

Virus scanning

Email is scanned for malicious content by the provider.

Anti-spam

Reputable email service providers filter spam messages from your in-box.

Phishing protection

Some service providers will identify potential phishing emails.

Look for a provider that offers enough storage, good IMAP and POP sync options for your mobile device and an intuitive interface.

password protection

Weaknesses stem from how users choose and manage passwords, which can make it very easy for hackers to access them and break into individual accounts.

Password management tools help users store and organize passwords and can even provide additional features, such as form filling and password generation.

FEATURES TO LOOK FOR

Synchronization

A good password manager will allow access from anywhere and synchronize across devices.

Password generator

Automatically generates strong, complex passwords.

Encryption

Passwords are stored encrypted, and the master password is not retrievable.

Multi-factor support

Better management tools will support complex multi-factor passwords.

Look for a password management tool that supports the types of browsers, operating systems and mobile devices you use.

virus and malware protection

If you use a computer for web surfing, shopping, banking, email and instant messaging and do not have proper protection, you are at high risk of being victimized.

Running real-time antivirus products and keeping them up to date is an essential step to reduce risks from malware and can reduce infection by more than 80%.

FEATURES TO LOOK FOR

Detection

High-quality software detects existing and new variations of malicious software.

Cleaning

Effectively quarantines or removes malicious software from an infected device.

Protection

Helps maintain a healthy system by proactively preventing malicious infection.

Performance

Good antivirus software will not slow down your system.

Parental controls

Optional feature that will secure your systems when used by children.

Backups

Many applications provide optional back-up protection in case of system failure.

Consider the number of devices that each vendor will allow the software installed on per license subscription purchase.

wireless routers

A wireless router allows you to connect devices to the internet and communicate with other devices on your network.

Routers are computers, with their own operating systems, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log keystrokes and access your accounts.

FEATURES TO LOOK FOR

Distributed Denial of Service (DDoS) protection

Prevents high-volume malicious attacks to your home network.

Guest network

Allows for separate network and credentials for temporary access.

Firewall

Secures your network from intrusion.

Look for a router with a range that fits the size of your home and supports the number of devices you want to connect to it.

SA-CYBSEC

J.P.Morgan
Asset Management