JPMorgan Chase & Co.

CYBER SAFETY

Cyber Top Tips*

Cyber crime continues to be a threat to individuals, families and businesses across the globe, making it essential to make good cyber practices part of our daily activities to avoid various cyber threats and potential fraud.

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

10 Key CYBER SAFETY Tips

1. Create separate email accounts for work, personal use, alert notifications and other interests
2. Be cautious of clicking on links or attachments sent to you in emails or in text mesages
3. Use secure messaging tools when transmitting sensitive information via email or text message
4. Create strong passwords and change them regularly
5. Do not use the same password for multiple accounts
6. Minimize the use of unsecured, public networks
7. At work, limit web usage to core, business-related sites
8. At home, set up a primary network and a separate one for guests, children and smart devices
9. Install anti-virus software on all your devices and keep it up-to-date
10. Be prudent in what you share about about yourself, family, job or business via social media

Email

- ✓ Use separate email accounts: one each for work, personal use, user IDs, alerts notifications, other interests
- ✓ Choose a reputable email provider that offers spam filtering and multi-factor authentication
- ✓ Use secure messaging tools when replying to verified requests for financial or personal information
- ✓ Encrypt important files before emailing them
- ✗ Do not open emails from unknown senders

Passwords

- ✓ Create complex passwords that are at least 10 characters; use a mix of numbers, upper- and lowercase letters and special characters
- ✓ Change passwords at least four times a year
- ✓ Consider utilizing a password management tool
- ✗ Do not use the same password for multiple accounts
- ✗ Do not click "Remember my password" or "Remember me" on websites you visit

Internet usage

- ✓ Download software only from trusted sources
- ✓ Log out of sites instead of simply closing the session window
- ✓ Look for https:// for secure session validation
- ✓ Enable private browsing whenever possible
- ✓ Delete cookies regularly
- ✗ Do not click on links from unknown or 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 and use biometric tools when available
- ✓ 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
- ✓ Review your privacy, location and password settings
- ✓ Pay attention to the information an app can access and regularly review permissions
- ✓ Enable remote automatic wipe in settings to ensure your personal information is erased automatically if you report your device as lost
- ✗ Do not click on ads when surfing the internet

Virus and malware protection

- ✓ Install anti-virus and ad-blocking software and keep it up-to-date
- ✓ Keep software, browser and operating systems up-to-date
- ✓ Regularly back up your data
- ✗ Do not install or use pirated software
- ✗ Do not install file-sharing programs
- ✗ Do not set email to auto-open attachments

Home networks

- ✓ Create one network for you, another for another for guests, children and smart devices
- ✓ Change the default password to your wireless network
- ✓ Turn on router's WPA2 encryption and firewall
- ✓ Enable "Do not broadcast" on your primary network's name (SSID) via the router software
- ✗ Do not use default router names/passwords

Public Wi-Fi/hotspots

- ✓ Minimize the use of unsecured, public networks
- ✓ Turn off auto connect to non-preferred networks
- ✓ Turn off file sharing
- ✓ When public Wi-Fi cannot be avoided, use a virtual private network (VPN) to help secure your session
- ✓ Disable ad hoc networking, which allows direct computer-to-computer transmissions
- ✗ Never use public Wi-Fi to enter personal credentials on a website; hackers can capture your keystrokes

Social engineering

- ✓ Confirm the identity of anyone requesting information or access to your data or devices via an alternate, verified method
- ✓ Limit the amount of personal information you post online
- ✓ Review privacy settings on social media accounts
- ✗ Do not open an attachment from someone you know if you are not expecting it; call to confirm before clicking
- ✗ Do not assume a request is genuine just because the requester knows information about you or your company
- ✗ Do not use personal information widely available on social media (pet's name, child's birthdate) to protect online accounts

When selecting services, software and equipment, consider the following:

Password managers

Weaknesses stem from how individuals 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

ENCRYPTION
Passwords should be stored with at least 256-bit AES encryption.

PASSWORD GENERATOR
Can automatically generate strong, complex passwords.

SYNCHRONIZATION
A password manager should allow secure access from anywhere and synchronize across devices.

MULTI-FACTOR AUTHENTICATION
Offers multi-factor authentication.

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

Virtual private network (VPN)

VPNs are a digital way of shielding your activity, much like using your hand to cover your PIN entry at an ATM. A VPN prevents prying eyes from seeing or tracking the contents of your communications

This is particularly important to use on personal devices when using public, travel, or an unsecured Wifi network.

DATA RETENTION
Look for a provider that does not retain your data logs, or web traffic.

OBFUSCATION
Provider should have servers across multiple countries to facilitate an IP assignment that is not easily traceable back to you.

COMPATIBILITY
Ability to install on desktops, tablets, and mobile devices.

REPUTATION
Reputable provider with a proven track record, with focus on security and ease of use.

Understand that VPNs will not protect you from viruses. Additionally, VPNs may be prohibited by some governments. Inform yourself before you travel.

Virus and malware protection

If you use a computer or mobile device for web surfing, shopping, banking, email and instant messaging and do not have adequate protection, you are a higher risk for becoming a victim.

Running real-time anti-virus products and keeping them up-to-date is an essential step to reduce risks from malware.

DETECTION
Should detect 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
Does not slow down your system.

PARENTAL CONTROLS
Optional feature to help limit content when devices are being used by children.

BACK-UPS
Optional back-up protection in case of system failure.

Consider the number of devices that each vendor will allow the software to be 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 like computers, with their own operating systems, software and vulnerabilities. If hackers gain access to your router, they can gain access to your files, log key strokes, access your accounts and can infect devices on your network.

AUTO-UPDATE
Choose a router that automatically updates its software, also known as firmware.

FIREWALL
Secures your network from intruders.

GUEST NETWORK
Allows for a separate and secure network and credentials for guests, children, and smart devices.

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.