cybersecurity awareness

WHAT TO DO

J.P.Morgan

Our commitment

J.P. Morgan devotes significant resources to maintaining the security of our computer systems, software, networks and other technology assets against attempts by unauthorized parties to access or destroy confidential data, disrupt service or cause other damage. Worldwide, nearly 1,000 employees are focused on our cybersecurity efforts, including working with local government and law enforcement agencies and other businesses to maintain our defenses and enhance our resilience to threats. These efforts will only intensify in the coming years.

Driving toward **a cultural shift**

The internet is woven into everything we do. Cybercrime is a growing and serious threat. These facts of life make it essential that all of us consciously make fraud prevention part of our daily activities.

These pages identify eight areas of serious vulnerability—and provide detailed steps to help protect yourself, your assets and personal information.

Passwords 6
Email 8
Internet 10
Wi-Fi hotspots 12
Home networks 14
Mobile security 16
Malware 18
Social engineering 20

Passwords are your first line of defense

Hackers use multiple dictionaries of English and foreign words, names and linguistic patterns to identify password roots. Their guessing strategies break two-thirds of all passwords existing today.

Create strong passwords

- Add complexity by combining upper- and lowercase letters, numbers and symbols.
  - Avoid using words that can be found in a dictionary.
  - Never use your name, social security number, address or other personal information (e.g., pet name) that can be easily found online.
- Go long—we suggest at least 10-14 characters.
  - Adding a “space” can make your password stronger.
- Create password tiers.
  - Use separate passwords for systems, user accounts and documents.
  - Change your passwords three to four times a year.
- Store passwords in a safe place or use a secure password management tool.

What to avoid

- Do not disclose your passwords online or give them to anyone.
- Do not store your passwords where they can be seen/found by others (e.g., on a Post-It note stuck to your computer).
- Do not click the “Remember My Password” option on various sites.
- Do not use the same password for multiple accounts.
- Do not create common passwords.
- Do not include profile or personal information posted on social media, networking or other internet sites.

long and complex is best

Avoid short and sweet passwords

The longer and more complex you make your password, the more secure it will be.

PASSWORD EXAMPLE	TIME TO CRACK
Rover	Instantly
R0ver	Instantly
Rover12	< 1 minute
@Rov3r12	< 1 minute
@Rov3r123	< 1 minute

Use a phrase instead of a word

Pick a phrase you will remember, such as: ***Rover went to market.***

Run the words together and:

- Capitalize some letters.
- Substitute numerals and symbols where it makes sense.
- Use acronyms, or abbreviate, as needed.

Or double a short password to increase length and strength.

PASSWORD EXAMPLE	TIME TO CRACK
Rov3rWENT2Mark3t	> 100 years
or try something like this:	
2BorNot2B_ThatIsThe?	> 100 years
4Score&7yrsAgo	> 100 years
Happy_Birthday_2_me	> 100 years
Rover12=Rover12	> 2 years

Create a password “root” and use it across all accounts

Using variations on a basic password “theme” can make it easier to remember. Do not use the same password for multiple accounts.

PASSWORD EXAMPLE	TIME TO CRACK
For e-commerce sites	
1LUV2_by_SHZ	> 2 years
For online banking	
1LUV2_uz_$$	> 2 years
For a car service	
1LUV2_uz_LIMOS	> 2 years

Sign up for a password management service

There’s only one master password to memorize: The system automatically creates a complex password anytime you need or change one.

Email providers can’t guarantee your cybersecurity

Hackers attack email providers to gain access to user accounts. Or they directly attack individual email accounts, using phishing, malware, social engineering and other scams.

Limit your exposure

Maintain at least four separate email accounts, as in the following examples:

For business
michael.pearce@businessname.com

For friends and family
michael.pearce@xmail.com

For important alerts
alerts4mike@xmail.com

For sites that require an email address as a user ID
gone2fish@xmail.com

In addition, to safeguard your information:

- Enable two-factor authentication in your email service when available to receive a text when there is a log-in from a new computer.
- Use data encryption to transmit personal information. Encoding the information makes it impossible for those without the encryption keys to read it.
- Employ spam filters to reduce the risk of malicious software and phishing scams (spam represents 66% of all email traffic[1]).

[1] Symantec 2014 Internet Security Threat Report, Volume 19.

follow an ongoing cybersecurity regimen

Routinely check email account settings

Criminals hacking into your account can change your settings to forward your mail to their own accounts.

Adjust email account settings

Prevent incoming images from automatically downloading.

Be selective with business and personal email addresses

Create separate email accounts: one for business, another for friends and family—and don't use them interchangeably. Share addresses with family, friends and trusted business associates on a need-to-know basis.

Do not email personal information

Social security or credit card numbers should not be sent over the internet.

Use strong and unique passwords

Create a 10-to-14-character password for every email account. Change it three or four times a year.

Access email only from secure networks

Avoid using public Wi-Fi hotspots.

Be alert to social engineering attempts

Scammers often counterfeit company logos, names and symbols to deceive unsuspecting individuals.

Keep corporate and personal email communications separate from each other

Don't conduct business through your personal email account, and vice versa.

Every device on the **internet** can be hacked

Hackers create clones of well-known websites to capture user credentials: the passwords, social security numbers, credit card information, etc. They then use the stolen information to access your banking and other accounts.

Precautions to take online

- Keep your browser software up-to-date.
- Maintain a medium or higher level of security on your browser settings.
- Make sure the web address of any e-commerce site or online banking service begins with **https://**.
  - Some browsers show a padlock icon next to the https:// to indicate a secure/encrypted connection.
  - Remember: **http://** is not secure.
- Log out after using an internet banking service to ensure your session has closed.
- Keep your data cookies and browser cache clear so that hackers cannot access your history and obtain information.
- Keep pop-ups and ads blocked, and never respond to pop-ups asking you to submit or resubmit your log-in information.
- Be mindful of the sites you visit:
  - Avoid sites that provide illegal downloads or illegal content (e.g., file sharing): Even if you do not download any files, you are vulnerable to viruses that can infect your computer. (This malware can attack your browser and change your home page without you being aware of it.)
  - Hackers increasingly target children on gaming websites.

What to avoid

- Do not download anything from unknown sources: Download/install software only from online sources you trust.
- Do not allow your internet browser or websites you visit to remember your passwords or credit card information.
- Do not link accounts across websites—in case one gets compromised:
  - Many sites allow you to log in using Facebook, Gmail, etc. Maintain separate accounts.

whenever possible

Regularly check your banking and credit card transaction histories

Also check statements for suspicious transactions.

Enable private browsing whenever possible

Prevent cookies and browsing history from being stored/saved to your device.

Use trusted bookmarks for important sites—not email links or pop-ups

Close windows containing pop-up ads or unexpected warnings using the X in the upper right-hand corner. Avoid clicking either the ad's "close" button or anywhere within the window to close it.

Do not buy anything promoted in a spam message

Even if it's not a scam, your purchase encourages spamming.

Use two-factor authentication when it's available

You confirm your ID in two steps each time you use an ATM—with a debit card and PIN. Do the same online: Use a password and a code sent to you via text, email or call to access your account. You will receive an alert if someone logs in from a new computer.

Wi-Fi hotspots are very convenient—and very dangerous

Hotspots and public Wi-Fi links have become popular with cyber criminals—who use them to collect log-ins, emails, payment information and more. Use public hotspots only if you absolutely must—and be sure to take the right precautions.

A very real danger

NEVER use a hotspot for banking or shopping transactions, or to send or store private information.

Use a Virtual Private Network (VPN) service to create a secure browsing session (i.e., to ensure that all of your data is encrypted as it passes through the network). VPNs are a low-cost way to create a baseline level of security on public Wi-Fi access points. Note: Most chat/IM sessions are NOT secure.

Disable ad hoc networking, which allows direct computer-to-computer transmissions, bypassing the router. This can allow an adversary to connect directly to your laptop and gain access to your computer and data.

Turn off file-sharing before you connect to a hotspot so that other users cannot gain access to your files.

Do not allow automatic connections to nonpreferred networks. Your device could be automatically connected to a public network, including those established for criminal purposes (e.g., to steal data).

Make sure a firewall is installed, and enable it before using a hotspot. Both Windows-enabled devices and Macs have built-in firewalls.

balance security with convenience

Every device is at risk

Laptops, smartphones and tablets are all susceptible to wireless security risks.

Use your mobile phone network

When you access websites that store or require sensitive information, use your mobile provider network instead of a public Wi-Fi connection.

Be suspicious of all Wi-Fi hotspots

Do not connect to sites you don’t know or recognize. Also, don’t assume a Wi-Fi link is legitimate: Hackers can create a fraudulent access point that’s identical to one that’s legitimate. Instead, use a Virtual Private Network (VPN), which allows only authorized users to access the network so data cannot be intercepted.

Protect all your devices

Install robust anti-malware and security solutions—and update them regularly.

Be aware of your surroundings

Internet cafes, libraries, airports, subways and other public places are popular with shoulder surfers: People who look over your shoulder to see what’s displayed on your screen.

A secure **home network** requires a secure router

Hackers can easily penetrate an open or insufficiently secured wireless network. Once inside, they can intercept your internet traffic and capture personal data, including the IDs and passwords you use online at banks, shopping sites and forums.

Limit your exposure

If your router is not well protected, a hacker can take control of it and pose as you (e.g., use your IP address) to commit a cybercrime—in addition to stealing your personal data:

- Every router is sold with a factory-default username and password. To put multi-layered protection in place, you should change your:
  - Router's default password
  - Router's name/SSID
  - Wireless network password
- Turn off your home's wireless network when it's not in use, thereby limiting the amount of time it is susceptible to hacking.
- Stop your router from broadcasting your home network's name (SSID). It is unnecessary and may invite unauthorized users to try and access your network.
- Use a network monitoring app to scan your network to see if you have unwanted users or devices on your network.
- Visit a site like www.onguardonline.gov for tutorials on how to adjust the security settings of wireless routers. You will find instructional videos from several manufacturers.

secure your router

Turn on encryption with a strong password

WPA2 is currently the strongest home encryption.
WEP is less secure and should never be used.

Turn on the router firewall

Wireless routers may be shipped with the firewall turned off. Make sure it is turned on.

Replace the router’s preset password

Most people forget to do this, but you should ensure that the router password is not the same as the one for your wireless network.

Change your router’s name or SSID—and create two networks

Create a guest network, identifying it as your primary network (e.g., Joe’s Network). Your guest network can have Wi-Fi access that is broadcast. Set up a secure network for yourself. Do not broadcast its name or give out its SSID to anyone. This network should have a name that cannot be easily guessed by others (e.g., TZPX3Y4).

Update the router’s wireless network password

This is called the network security key. Have one for both guest and secure networks.

Keep your router’s firmware up-to-date

Install all security patches. Replace your router every three years (firmware is not always updated by the manufacturer on older routers).

Have strong passwords on all devices connected to your network

Smart TVs, home security cameras, printers, thermostats, etc., all need to protect against unwanted external access.

Establish secure guest and personal networks

Netgear, Linksys and Apple Airport all support additional guest networks.

Mobile devices are under increased attack

As we all become more dependent on smartphones and tablets for banking, shopping and social networking, it's critical to protect your mobile devices.

Precautions to take

- Adjust your security settings to restrict others' access to your data via wireless and Bluetooth connections.
- Avoid clicking on ads: Ad-blocking apps exist for both Android and Apple devices, and browser settings can be adjusted to limit ad-tracking.
- Download an app such as *MyPermissions–Privacy Shield* (available for iOS and Android), which will scan your device and tell you which apps are accessing your information.
- Update the apps on your device when new versions become available, as these often include security patches.
- If you think your device has been infected with malware:
    - Contact either the device maker or your mobile phone carrier for help.
    - Install a security app to scan and remove malware-infected apps.
    - Do not try going into the device's operating system (e.g., don't jailbreak or root your phone). This lessens the device's security level/protection.

secure your mobile devices

Keep your phone or computer locked

Make sure it is password protected at all times.

Keep the device's operating system software up-to-date

Ensure you have the latest security patches.

Encrypt sensitive information

If your mobile device or laptop has data encryption features, use them.

Monitor how apps behave on your phone

Keep track of permission access/requests from apps installed on your device. Download an app such as *MyPermissions–Privacy Shield* to scan your device.

Use a reputable anti-malware/virus program and update regularly

Mobile devices are susceptible to the same risks as your home/office computers.

Turn off Bluetooth when you don't need the connection

Your device will be less vulnerable both to cyber attacks and a drained battery.

Choose a smartphone with anti-theft security features

If your phone is lost or stolen, having remote access to it will allow you to lock it, wipe the data stored on it and identify its location.

Back up your mobile devices

Regularly backing up to your home computer or cloud network ensures you will have access to information if your device is lost, stolen or corrupted.

Malware is a serious and persistent threat

Criminals use malware to steal or destroy your data—in the process, compromising the security and integrity of the equipment and/or systems you use.

Things aren't always what they seem

- **Don't ignore the warnings.** Install anti-virus software and pay attention to warnings you receive, such as when you are trying to access an unsafe site on the internet.
- **Be careful what you click and download.** Clicking unfamiliar links can expose you to malicious software programs that scan your computer or track keystrokes, including passwords and account numbers.
- **Some programs intentionally include malware.** When installing, pay attention to message boxes and the fine print. Cancel any installation if you believe it may be harmful.
- **Be wary of suspicious-looking email.** Even email from people you know can contain malware links or attachments if their accounts have been compromised.
- **Be careful following links in incoming email.** Whenever possible, visit websites by entering the desired address directly in your browser.
- **Scan files with security software before opening.** Do not assume emailed files or those given to you on a disc or flash drive are safe.
- **Do not trust pop-up windows asking you to download software.** Their goal is to convince you that your computer has been infected and that downloading the software will take care of the problem. Close this window immediately, making sure not to click on anything inside the pop-up window.
- **Most file-sharing sites are illegal and should be avoided.** There is very little policing for malware in these types of services. Malware can be disguised as a popular movie, album or program.

reduce your risk of a malware infection

Keep your security software, web browser and operating systems up-to-date

Install anti-virus and anti-malware software only from a trusted source

Regularly update your software and scan your system often.

Turn on automatic updates

Take advantage of this valuable anti-virus software option.

Make sure your firewall is ON

Update settings to maximize protection for all network locations—home, work, public.

Do not install software you did not specifically seek out

Do not download software from untrustworthy or unknown sources. Remove/uninstall software you are no longer using.

Avoid using USB and other plug-in devices

It's impossible to know if a USB device is completely safe. Use online storage as an alternative.

Back up computer data

Use a CD, DVD or network to ensure you have access to your information in the event your computer or mobile device becomes corrupted.

Watch what you click

Do not click on links in pop-ups or spam—even those claiming to offer anti-virus software. They may also install spyware.

Social engineering can leave you vulnerable to fraud

Social media, such as Facebook or LinkedIn, can give hackers a wealth of information about you—which can be used to steal your assets or information.

Guard against social engineering online

- **Limit the information you give out.** Criminals will search Facebook, Twitter and other social media for information about you and use it to defraud you, your family and/or your friends.
- **Don't put personal/financial information** in emails (or follow links sent to you in emails even if they come from trusted sources).
- **Contact the email sender by phone** or a new email window (do not hit "reply") to ask the sender if the email you received is valid.
- **Pay attention to the URL.** Malicious websites look identical to real ones, but the URL may use a spelling variation or different domain. (For example, does it say .net when it should say .com?)
- **Don't enter sensitive information** on websites unless you see proper security (the URL should begin with: https://).

And via telephone

- **Confirm an unknown caller's identity:** Ask for the full and correct spelling of their name, a call back number, and an explanation for why the information is needed.
- **Be wary of impersonators:** Validate the source through official public channels.
- **Do not supply information about other people:** Have the caller contact the appropriate individual directly if you are asked for someone else's information.

vigilance is the best defense

Google yourself

See what information is available about you online—and limit it. Use website privacy settings to avoid widely sharing your information.

Verify callers' identities

Contact a company/organization directly if you receive a call from an unknown representative.

Be alert to phishing attempts

These take many forms, including: attachments you haven't asked for; directives to change your password to something specific, such as 12345; and/or payment instructions to a new address.

Recognize the warning signs of fraudulent email

Poor grammar, misspelled words, overuse of capital letters, urgent or threatening language, sender names/addresses that are vague or incorrect are all indicators that something is wrong.

Defend against having your email hijacked

Even if the sender is someone you know, if you unexpectedly receive an email with a link or attachment, contact the sender to verify authenticity before opening links or downloading content.

Do not automatically follow payment instructions you receive in an email

First validate the instructions, either by telephone or in person.

Keep your software up-to-date

Hackers use social engineering techniques to test if software or security measures are out-of-date, and exploit those weaknesses.

If you think your accounts have been compromised:

- Contact your financial institutions immediately and close the accounts
- Check for unknown charges
- Immediately change your passwords

We can help

Please contact your J.P. Morgan team at once if you believe your identity or personal information has been stolen, or if you think your accounts have been compromised in some way.

This document is provided for educational and informational purposes only and is not intended to address every aspect of the subject discussed herein. Any reproduction, retransmission, dissemination or other unauthorized use of this document or the information contained herein by any person or entity is strictly prohibited.