WELLS FARGO

Wealth & Investment Management

Navigating Today's Cyber Threat Landscape: Best Practices for Securing Your Digital World

Cyber Client Advisory
Cyber Resiliency & Human Defense, Wells Fargo Bank, N.A.

Investment and Insurance Products are:

- Not Insured by the FDIC or Any Federal Government Agency
- Not a Deposit or Other Obligation of, or Guaranteed by, the Bank or Any Bank Affiliate
- Subject to Investment Risks, Including Possible Loss of the Principal Amount Invested

© 2026 Wells Fargo. All rights reserved. PM-10312027-5448832

Today's Speaker



Justin Ellerman

Executive Director

Head of Cyber Client Advisory

Wells Fargo Cybersecurity

- 18 years of cybersecurity and privacy experience in financial services industry
- Previous roles include incident response, privacy operations, and cybersecurity strategy
- Holds an MBA and industry certifications including the CISSP, CIPP/US, GCCC, GCTI and GSTRT

Agenda

- Current threat landscape
- Motivations and methods of cybercrime
- Anatomy of a cyber scam
- Top cyber fraud tactics
- Cybersecurity at Wells Fargo
- Ways to help protect yourself and family
- Cyber hygiene checklist



Threat Landscape: The sobering facts

74%
Of breaches will have a root cause of the human element[2]

89%
Increase in attacks by AI-enabled adversaries[4]

900%
Annual growth of deepfakes in 2025[2]

$7.7 billion
Lost to scams by adults age 60 and older in 2025[5]

$15.63 trillion
Estimated annual cost of global cybercrime for 2029[3]

$1 billion
Stolen in “Phantom Hacker” scam targeting seniors[6]

Cybersecurity awareness training can lead to a **70%** reduction in security-related risks.[7]



Sources:

1. Sentinel One - Key Cyber Security Statistics for 2026, 2026
2. Fortune - 2026 will be the year you get fooled by a deepfake, researcher says., 2025
3. Statista -Estimated cost of cybercrime worldwide 2018-2029 , 2026
4. Crowdstrike – Global Threat Report, 2026
5. FBI 2025 Internat Crime Report, 2025
6. AG New York – Three Phase Scam Targeting Seniors 2025
7. Keepnet – Security Awareness Training Statistics 2026

Motivations and methods of cybercrime

Threat Actors	Goals	Attack Vectors
Who: ➢ Cybercriminals ➢ Hacktivists ➢ Nation-states ➢ Malicious insiders	**Why:** ➢ Theft • Financial gain • Personal data ➢ Disruption ➢ Espionage ➢ Reputation damage ➢ Attention ➢ Revenge	**How:** ➢ Phishing ➢ Social engineering ➢ Credential theft ➢ Infostealer malware ➢ Ransomware ➢ Vulnerabilities ➢ Denial of Service



Anatomy of a Grandparent Scam

1. Find a Target

Scammers often use social media, public records, or previous data breaches to identify elderly individuals and their family connections.

2. Build a Trap

The attacker crafts a believable story – often involving a grandchild in distress (arrested, stranded, hospitalized).

3. Send the Bait

The scammer initiates contact by phone, text, or email impersonating the grandchild or an authority figure (police officer, lawyer, doctor).

4. Break In

The scammer gains trust by exploiting emotions and urgency, convincing the victim to act quickly.

5. Take Control

The scammer directs the victim to the payment method or location, often staying on the line to ensure compliance.

6. Steal

Once payment is made, the scammer disappears. The money if often untraceable.

WHAT TO LOOK FOR

- Sudden contact from **someone claiming to be a relative** but sounding unfamiliar.
- Emotional urgency or secrecy: **“Don’t tell mom or dad.”**
- **Caller ID is blocked** or spoofed.
- **Messages claiming to be from grandchild** but sent from unfamiliar addresses.
- **Caller remains on the phone** during the financial transaction.
- **No follow-up** from the supposed grandchild.

WHAT TO DO

- **Hang up** from the scammer immediately
- **Do not send any money**
- **Contact your family member** using a known phone number
- **File a report** with local law enforcement
- **Submit a complaint** to the FTC at reportfraud@ftc.gov

Top Cyber Fraud Tactics for 2026

1

AI voice cloning and deep fakes

AI technology (i.e., AI-enabled chatbots, deep fakes) being **used to automate individual interactions** and other cyber fraud attacks at a **cheap and scalable** rate, which could increase the size, scale and speed of cyber threats.

2

Spoofing and Phishing

Emails or phone calls appearing to be from a known contact who trick targets into taking action directed by an attacker.

The FBI identified **$77 million in losses from phishing and spoofing scams impacted adults ages 60+ in 2025**.[1]

3

Tech Support Scams

A warning about a virus pops up on your computer with a number to call for help.

You end up paying hundreds of dollars to a scammer who "deals" with the fake virus.

Beware of scammers remotely accessing your computer.

4

Imposter Scams

Involve fraudsters **pretending to be someone you trust**, such as a government official or a company representative, to **steal your money or personal information by using fake emergencies or opportunities.**

5

Search Engine Manipulation

Cybercriminals are tricking search engines into showing fake customer support phone numbers in AI-generated summaries.

These scams harvest sensitive data during calls to bypass traditional security.

Beware of: Refusal to meet in person, Unexpected emails or texts, Suspicious search results, Promises too good to be true

1. FBI Internet Crime Report 2025

Cybersecurity at Wells Fargo

To help protect your assets and data from evolving cyber threats, Wells Fargo utilizes a comprehensive defense strategy that includes multi-layered security, constant monitoring, and swift response.

Our commitment:

- **Human Cyber Defense**
  Ensuring our staff are well equipped to recognize and respond to cyber threats.
- **Advanced Threat Protection**
  Utilizing cutting-edge technologies to identify and neutralize threats before they can impact our systems.
- **Proactive Defense**
  Implementing preventative measures based on real-time threat intelligence and industry best practices.
- **Robust Incident Response**
  A dedicated team to respond swiftly and effectively to any security incident.
- **Cyber Client Advisory**
  Providing you with knowledge and tools to help protect yourselves in the digital world.

24/7 Real-Time Monitoring & Response

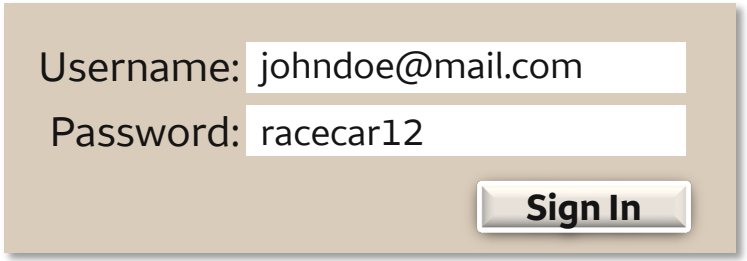
When it comes to the real world, attackers can get it right once - we must get it right…
Every Minute of Every Day



*Over a 30-Day Period

Helping protect yourself and your family

Better protect your online accounts



Create secure passwords.

- Strong passwords should be 12-16 characters minimum.
- A combination of upper- and lower-case, numbers, and special characters.
- Never reuse passwords across multiple websites.
  - If attackers obtain one password, then they have all of them.
  - Credential stuffing and dictionary attacks.

Consider using a password manager.

- Safely store all your passwords with one, secure master password.
- Maintain unique passwords for every website.
- Use a strong master password of 20-24 characters.

Protect your accounts with 2-factor authentication.

- Require a code sent via SMS, email, or a token to sign into your accounts.



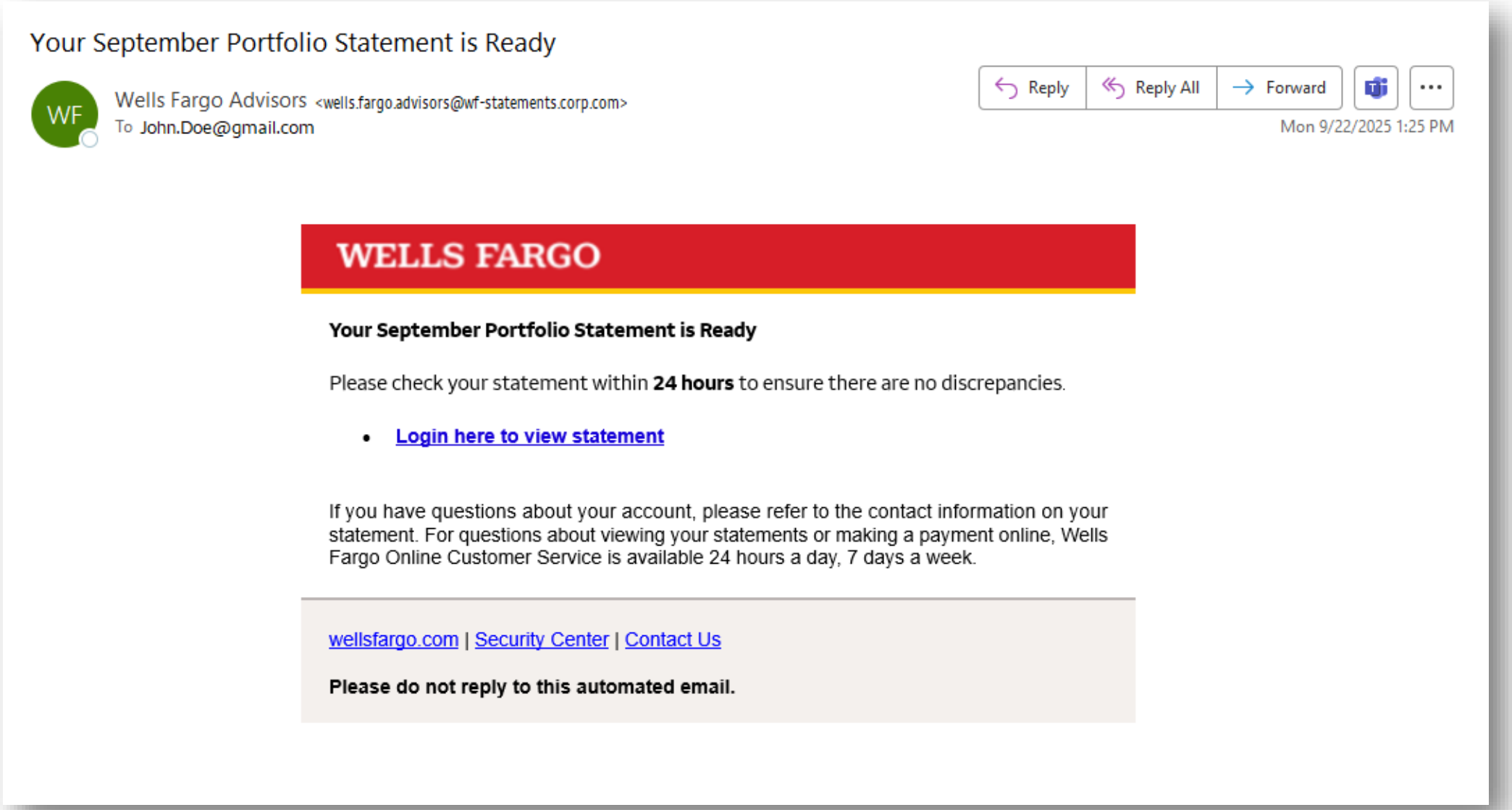
Password Brute Force Tolerance[1]

- 10 characters, numbers only — **Instantly**
- 10 characters, lowercase only — **1 minute**
- 10 characters, upper and lowercase — **21 hours**
- 10 characters, #’s, upper and lowercase — **5 days**
- 10 characters, #’s, symbols, upper and lowercase — **2 weeks**
- 12 characters, #’s, symbols, upper and lowercase — **226 years**
- 14 characters, #’s, symbols, upper and lowercase — **1 million years**
- 16 characters, #’s, symbols, upper and lowercase — **5 billion years**

1. Hive Systems Password Table

Spotting a phishing email – Test your ability

Is this email legitimate or not? **Do you see anything suspicious?**



Your September Portfolio Statement is Ready

WF

Wells Fargo Advisors <wells.fargo.advisors@wf-statements.corp.com>

To John.Doe@gmail.com

Reply | Reply All | Forward

Mon 9/22/2025 1:25 PM

WELLS FARGO

Your September Portfolio Statement is Ready

Please check your statement within **24 hours** to ensure there are no discrepancies.

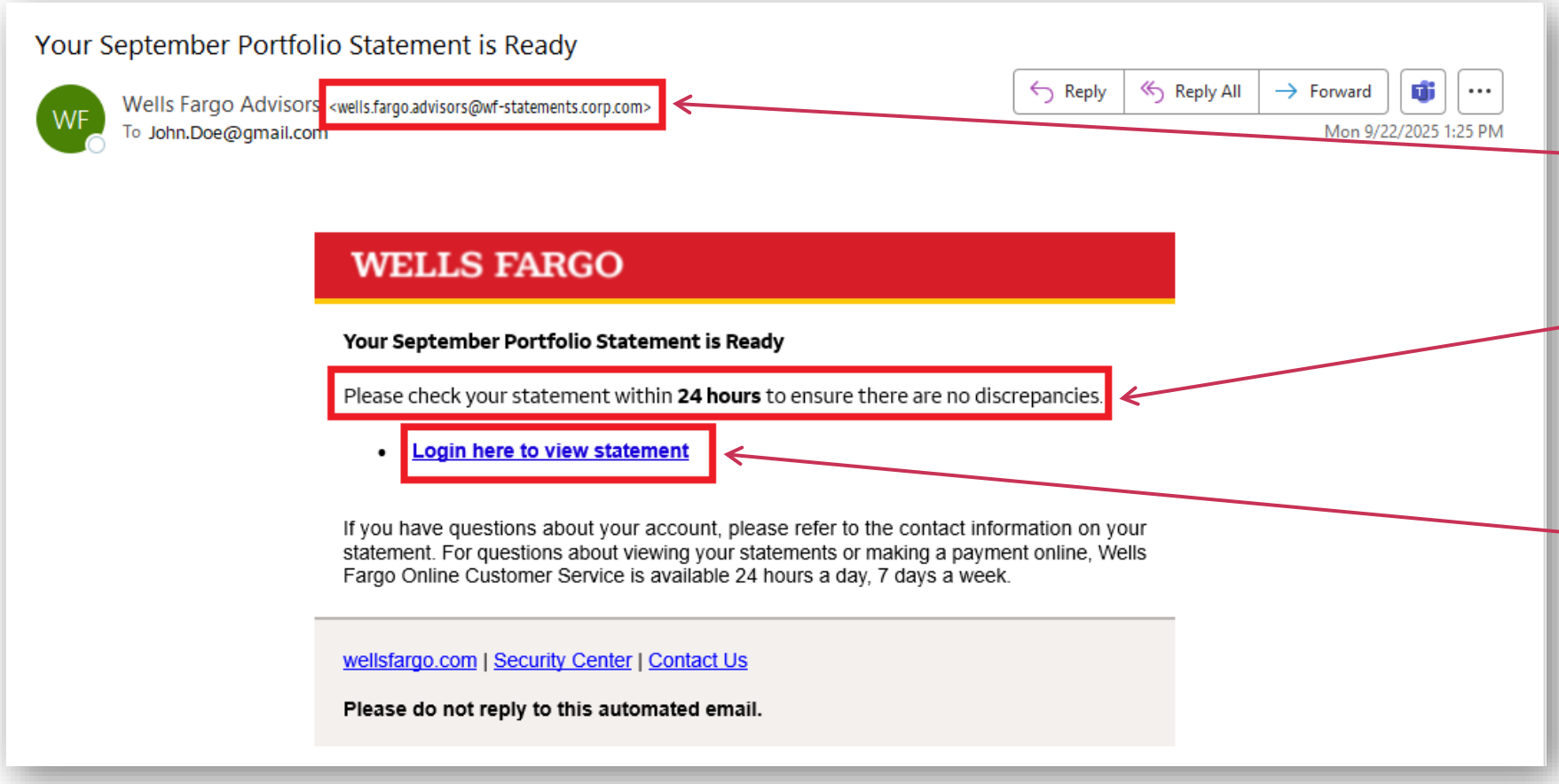
- **Login here to view statement**

If you have questions about your account, please refer to the contact information on your statement. For questions about viewing your statements or making a payment online, Wells Fargo Online Customer Service is available 24 hours a day, 7 days a week.

wellsfargo.com | Security Center | Contact Us

Please do not reply to this automated email.

Spotting a phishing email – The answer



Red Flags

- The sender's domain ends with **wf-statements.corp.com** instead of wellsfargo.com
- The message creates a sense of urgency by stating **Please check your statement within 24 hours**.
- If you hover over the link with the cursor, you will notice a suspicious URL to **wfstatements.corp.com/login**

Pro Tips

- Did you expect this message?
- Verify with your advisor through an established communication channel (like a phone call).

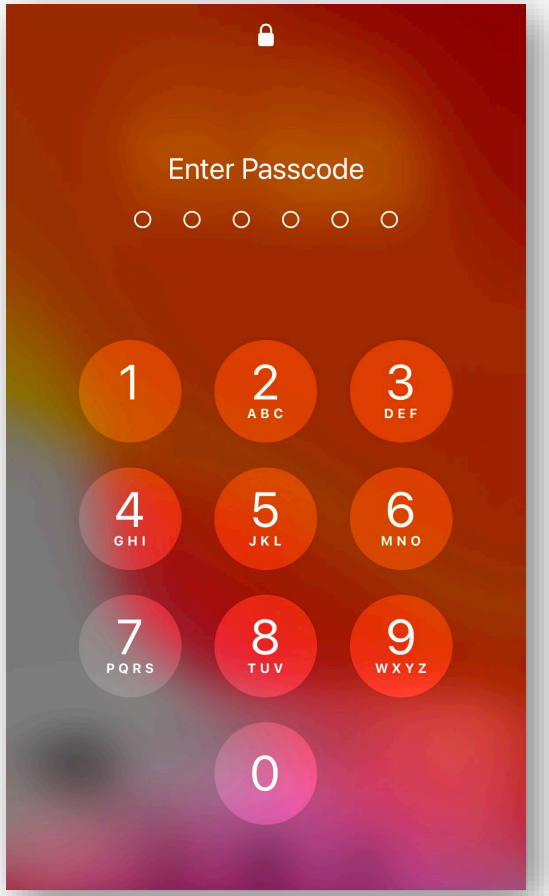
Mobile device security

Protect your device if it is ever lost or stolen

- Implement a passcode of at least 6 digits to encrypt your data.
- Enable “Erase after 10 failed passcode attempts”
- Turn on biometrics such as fingerprint or face identification.

Review your privacy settings

- What information displays on your phone when your phone is locked?
- Where are you sharing your location?
- Which apps can access your contacts or photos?



Mobile device takeover a.k.a SIM swap attacks

- Ask your mobile carrier to place a verbal PIN on your account in order to make changes.
- Contact your mobile carrier immediately if you stop receiving calls or texts.
- Enable additional protections your mobile carrier may offer to help protect against mobile device takeover.

Malware and virus protection

Ensure anti-virus software is installed on all your devices.

- Choose a provider that is compatible with all your devices (e.g., Windows and Mac).
- Anti-virus software should automatically update to help protect you from the latest threats.

Help protect yourself from Remote Access scams.

- Be on alert for spam calls and texts claiming something is wrong with your accounts or computer.
- Never allow remote access to your computer by someone you don’t know.
- Should you fall victim to a remote access scam, contact your bank immediately.



What is a remote access scam?

Cybercriminals pose as IT support or bank customer service and attempt to persuade you into giving them control over your computer to fix a problem that does not exist.

Once they have control of your computer, they can steal your identity and install malware to commit fraud a later time.

Artificial Intelligence (AI) Threats

Types of AI-enabled scams.

- AI-generated phishing emails from financial advisors, attorneys, business partners, or trusted contacts
- AI-generated documents, invoices, or wire instructions that appear authentic
- Voice clones of family members or others requesting urgent money movement
- Deepfake videos impersonating advisors or executives to authorize transactions

Help protect yourself from AI-enabled scams.

- Treat all unexpected “urgent” request for money, sensitive information, or credentials as suspicious
- Implement independent verification and call-back verification for financial requests
- Establish codewords with family or trusted contacts for verification
- Limit public audio or videos that can be used for AI scams



How is AI voice cloning used?

Cybercriminals create convincing AI-generated audio to use against intended targets. Victims may receive a phone call from someone that sounds and speaks like a family member or a trusted contact to trick the victim into taking urgent action such as revealing sensitive information or moving financial assets.

Use **independent verification** with pre-established phone numbers or **codewords** to help protect against these AI-enabled scams.

Help better secure your social media accounts

Even if you do not use social media…

- Remember your friends or family members may be posting information about you on their social media pages.

Review each site's security and privacy settings.

- Who can view your posts and profile?
- What information can be found through search engines?
- Enable 2-factor authentication, where available.

Limit sharing of personal details on social media sites.

- Information like your location, upcoming vacation plans, and personal data (e.g., birth date, anniversary date) can be used by cybercriminals to target you.

Monitor data broker and people-finder sites.

- Search for your personal data on these sites and request removal. (e.g., truepeoplesearch.com).

Be aware search engine operators can be used to find your social media content.

- Search operators help refine targeted searches on social media platforms by combining or excluding keywords.
  (e.g., **"**YourName**" site**:instagram.com **NOT** facebook.com)
- Proactively searching your own data using search operators can help identify security gaps.



Do you use professional social media sites like LinkedIn?

Cybercriminals use professional social media sites to identify which employees to contact when they are targeting a business.

Limit the amount of information you share about your job online.

Identity theft and fraud

Review your credit file regularly.

- You can obtain your credit report annually from the 3 major credit bureaus for free on www.annualcreditreport.com .

Implement credit freezes.

- Restrict access to your credit file at each of the 3 major credit bureaus with a credit freeze.
- Help protect those you care about with a credit freeze, such as children and elderly family members.

Consider a credit and identity monitoring service.

- Be alerted of potentially suspicious behavior occurring on your existing accounts .
- Access identity theft recovery experts should you experience fraud.



Change the answers to your vetting questions

Don’t protect your identity and wealth with easily found or guessed information about you

Mother’s maiden name: Grapefruit

Favorite vacation spot: Kiwi

Victim of Identity Theft?

Report it immediately to your financial institutions as well as the FTC at www.identifytheft.gov

Top 10 cyber hygiene checklist

By embracing these cyber hygiene practices, you directly contribute to a stronger, more resilient you that helps protect not only yourself but also your loved ones in an increasingly digital world.

1. Strengthen your passwords

- ✓ Use unique, complex passwords combining uppercase, lowercase, numbers, and symbols
- ✓ Consider using a passphrase
  - Typical password example (P@ssword123)
  - Passphrase example (Sunsets!OverTheRockyMountains2025)

2. Activate multi-factor authentication (MFA)

- ✓ Enable MFA on all work and personal accounts for another layer of security beyond your password

3. Spot & report phishing attempts

- ✓ Be suspicious of unexpected emails, texts, or calls
- ✓ Never click suspicious links or download attachments

4. Verify urgent requests (especially financial)

- ✓ If you receive an urgent request for money, sensitive information, or change in payment instructions, always verify verbally with a trusted phone number

5. Keep all software updated

- ✓ Install updates on your operating system, applications, and browsers as soon as they are available

6. Be cautious on public WiFi

- ✓ Avoid accessing sensitive information or conducting business on public WiFi
- ✓ Always use a Virtual Private Network (VPN) for secure access

7. Secure your devices

- ✓ Always have strong passcodes and encryption enabled
- ✓ Always lock your device when stepping away

8. Think before you click or scan

- ✓ Always pause to think before clicking any link or downloading an unexpected attachment
- ✓ Before scanning a QR code, evaluate its legitimacy and determine if it's from a trusted source

9. Protect sensitive data

- ✓ Never share confidential information with an unauthorized individual

10. Regularly backup important data

- ✓ Regular backups are the best recovery plan against data loss or system failure
- ✓ Use a cloud service or external hard drive

WELLS FARGO

Wealth & Investment Management

Thank you

Wells Fargo provides best practice information related to cyber risk and/or topics for educational and information purposes only. This document is not intended to and should not be relied on to address every aspect of the risks discussed herein. The information provided in this document is for the purpose of helping customers and clients better protect themselves from cyber risk and highlight industry best practices for operating in a more secure manner. This document does not provide a complete list of all cyber threats or risk mitigation activities, nor does it document all types of best practices. Wells Fargo is not providing cyber-related advice or consulting services and customers and clients should decide whether to engage a cybersecurity firm for specific questions or advice. It is the responsibility of our customers and clients to determine their best approach for mitigating cybersecurity risk through implementation of best practice aligned to the level of risk.

Private Wealth is an exclusive and personalized service and product offering for qualifying clients of Wealth & Investment Management (WIM). WIM offers financial products and services through bank and brokerage affiliates of Wells Fargo & Company.

Wells Fargo Advisors is a trade name used by Wells Fargo Clearing Services, LLC (WFCS) and Wells Fargo Advisors Financial Network, LLC, Members SIPC, separate registered broker-dealers and non-bank affiliates of Wells Fargo & Company. WellsTrade® and Intuitive Investor® accounts are offered through WFCS.

© 2026 Wells Fargo. All rights reserved. PM-10312027-5448832