AVOIDING SCAMS
STAYING SAFE ONLINE

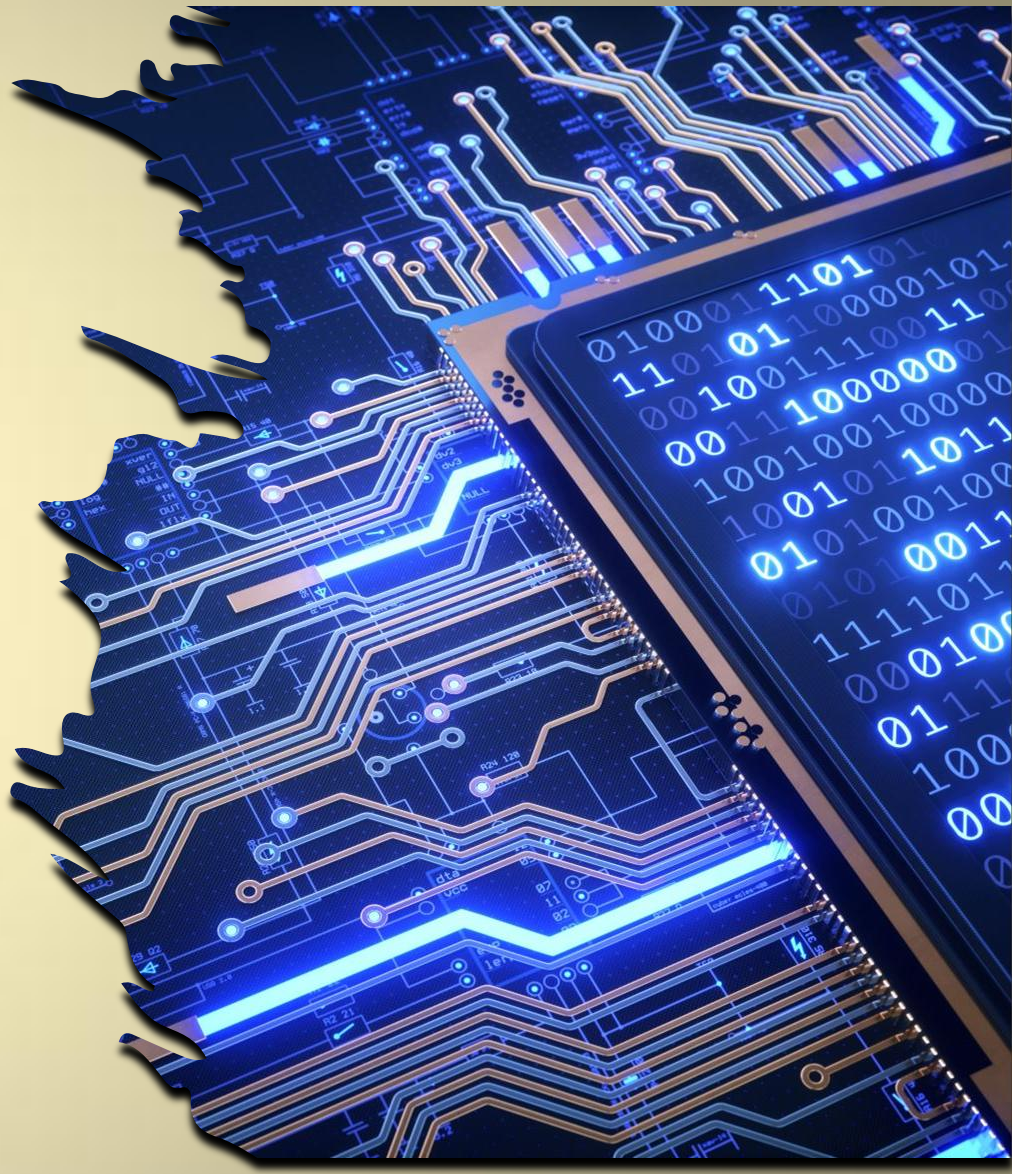
LOS ALTOS HILLS TECHNOLOGY COMMITTEE

AMEESH DIVATIA (CHAIR)
ANNIE JU (VICE CHAIR)
ANDREAS BIBL
AUGUSTIN FARUGIA
LEW JAMISON
GEORGE LEE
JOHN SWAN
SAM WOOD
RAJIV BHATEJA (VICE MAYOR)

DECEMBER 6, 2025

Agenda

- Introduction to Scams
- Reducing Risk and Password Safety
- Identifying and Avoiding Scams
- Protecting Accounts and Devices
- Recommendations and Additional Resources



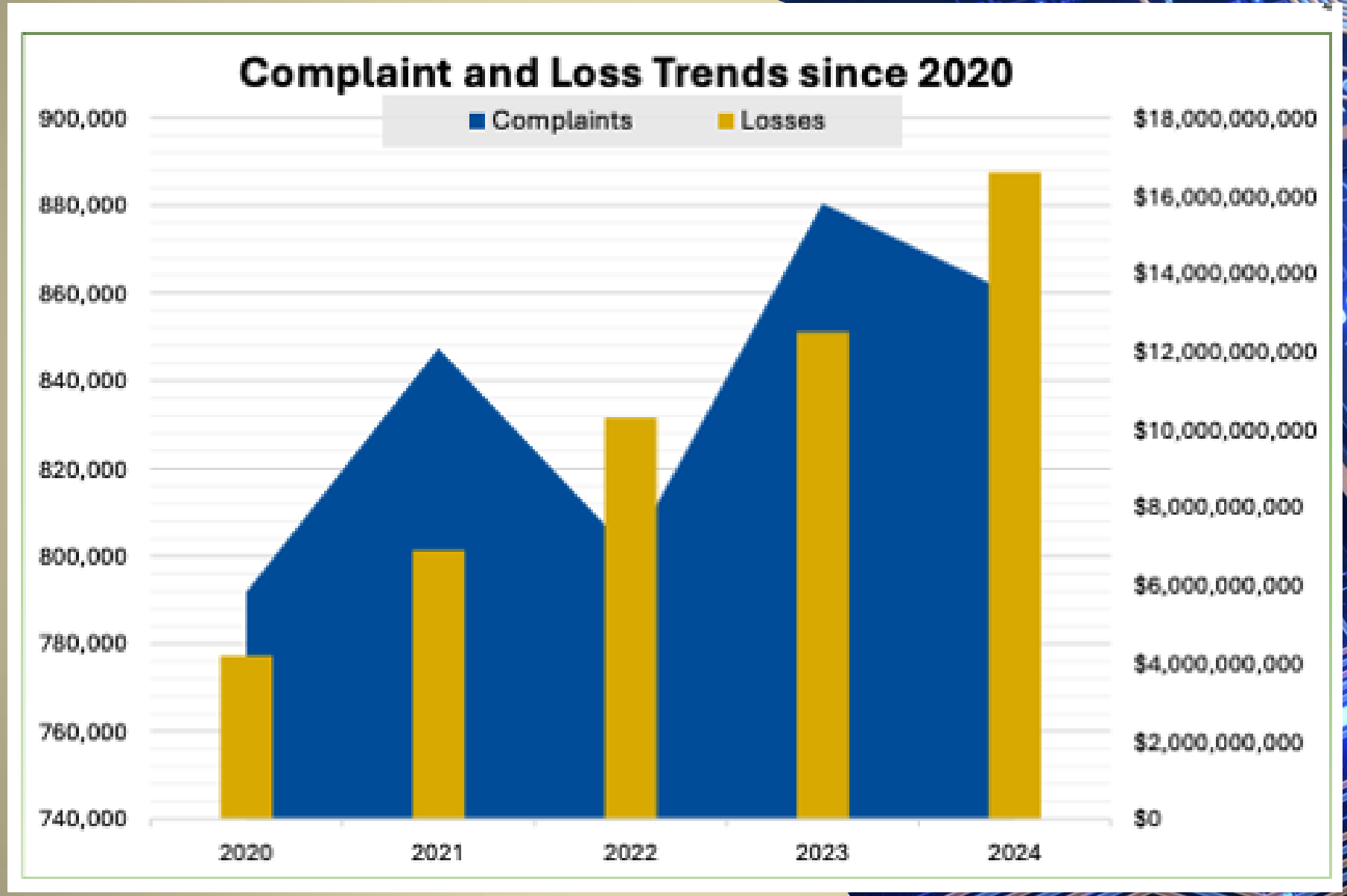

Scams

What You Can Do

- Be informed
  - Types of scams
  - Examples of online scams
  - Scammer tactics
- Reduce your risk
  - Safeguard your personal information
  - Harden your accounts
  - Increase your awareness
  - Reduce the risk of being scammed
- If you're a victim:
  - Whom to contact
  - Where to get help


Be Informed

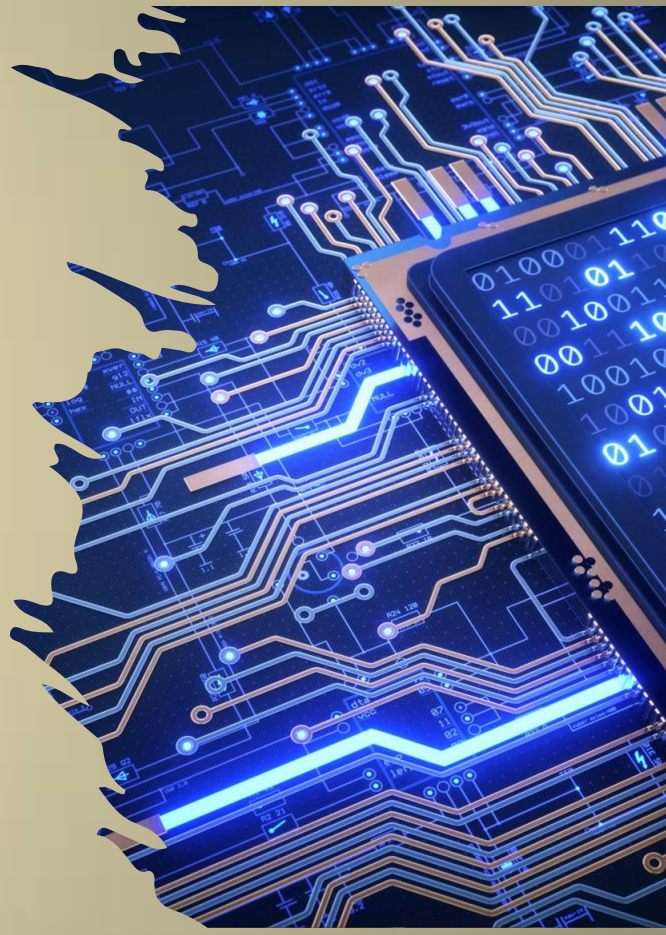
Growth of Scams



Source: FBI's Internet Crime Complaint Center (IC3)

Types of Scams

The Grandparent Scam
The Tech Support Scam
Person in Need Scam
Charity Scam
Online Romance Scam
Lottery/Sweepstakes/Inheritance Scam
Rental Scam
Government/IRS Impostor Scam
Online Shopping Scam
Mystery Shopper/Fake Check Scam
Employment Scam
Phishing
Vishing
Smishing



Excellent description of these on:
https://corporate.walmart.com/privacy-security/fraud-alerts


Reducing Risk and
Password Safety

Reducing Risk of Scams

Here are some ways of reducing risk:

- Be wary of **phishing emails,** fake online marketplaces, **FAKE BILL PAYMENT!**
- **Don’t click on links in emails**. Hover your cursor or go to the site directly.
  - e.g, https://wellsfargo.com actually points to scam.com
- Avoid **advance payment** scams and protect against **SIM swaps**
- Be skeptical of **beneficiary claims** and **grandchild in trouble** scams
- Use **password safety** practices like **Multi-Factor Authentication** and **password managers**
- Set up **alerts** and **credit freezes** for financial accounts
- Protect your devices and accounts with strong security measures

Protect Your Passwords

Create strong, unique passwords

- Use at least 12 characters, the longer the better.
  - Combine upper and lowercase letters, numbers, and special symbols.
  - Avoid using personal information (names, birthdays, or addresses).
  - Use a unique password for every account.
- Avoid using dictionary words or common phrases.

Enable Multi-Factor Authentication

- Verification code from app or text message.

Be wary of unsolicited phone calls and emails

- iPhones can silence calls from unknown numbers.
- Android can screen calls, and identify/ignore spam calls/texts

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Password Recommendations

1. Use UNIQUE passwords.

Never re-use important passwords

2. Use LONG passwords.

Use a password manager to generate strong passwords

3. Use MFA where available.

Multi-Factor Authentication: Authenticator App (preferred), or Text PIN

4. Have I been Pwned?

Is your password compromised?

Check:
https://haveibeenpwned.com/passwords

Use a Password Manager

Safer trend: Passkey…

Password Managers

Independent
- NordPass
- 1Password
- Dashlane
- Keeper
- Bitwarden
- LastPass
- KeePass

Browser-base
- Google Ch
- Microsoft
- Apple Safar

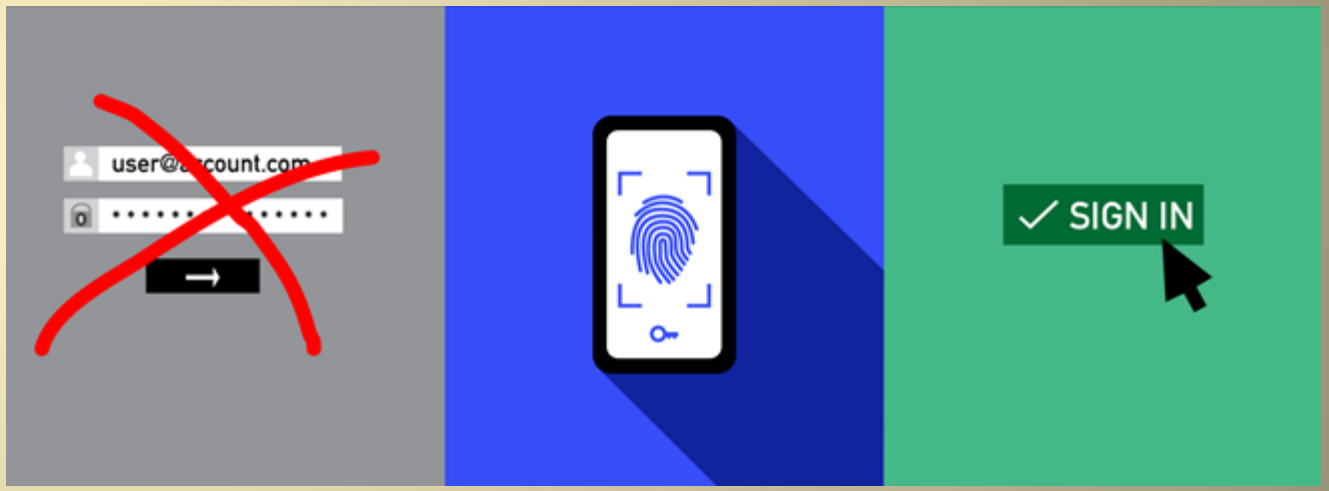
Smart Guessing Algorithm Cracks 87 Million Passwords In Under 60 Seconds

Password Manager suggested passwords are completely random and are harder to crack!

Password r **credentials.**
Ex
Password managers also advise you if your password has been hacked or is not secure.
Password managers also suggest very strong passwords.

What is a Passkey?

- A passkey is a password-less way to authenticate
- "Your device IS your password"
- Your device needs to be protected by a screen lock (fingerprint, PIN, pattern, etc.)
- Advantages:
  - No passwords to remember,
  - No password to hack
- But:
  - Protect your devices
  - **If someone gets access to your unlocked device…**

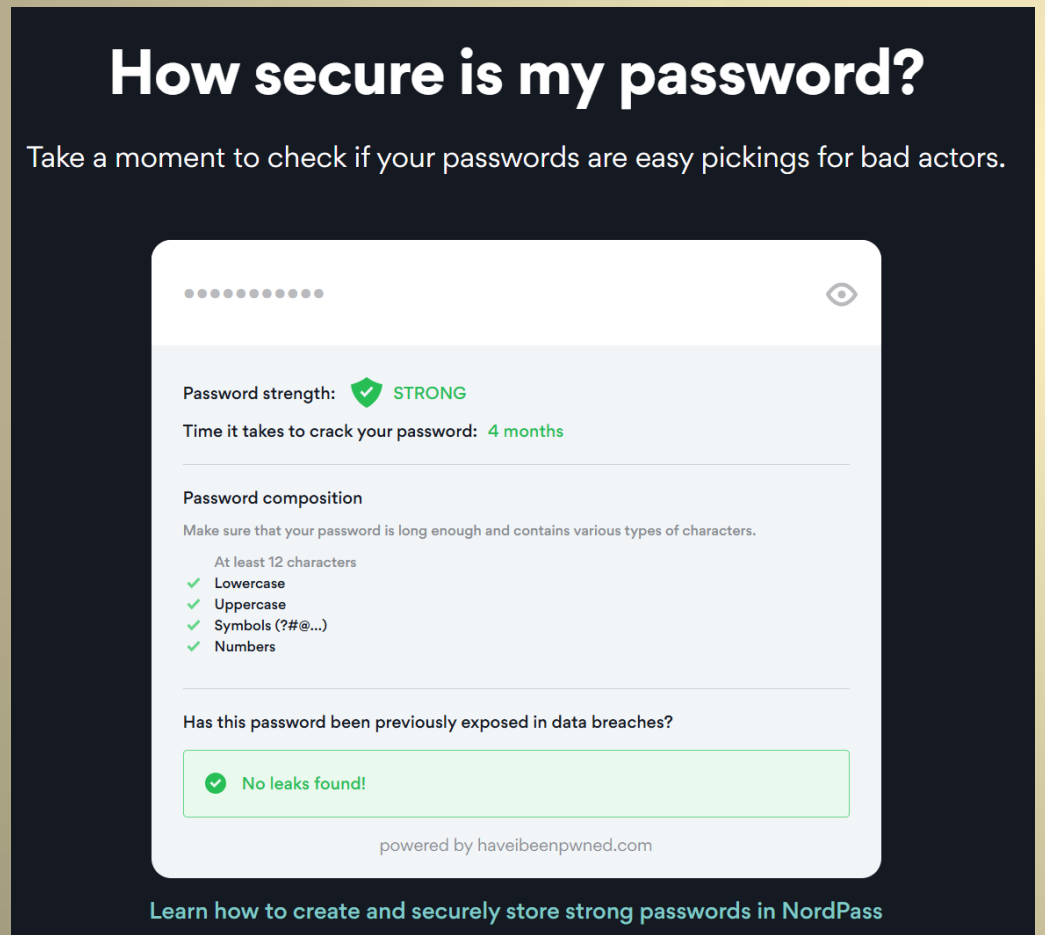


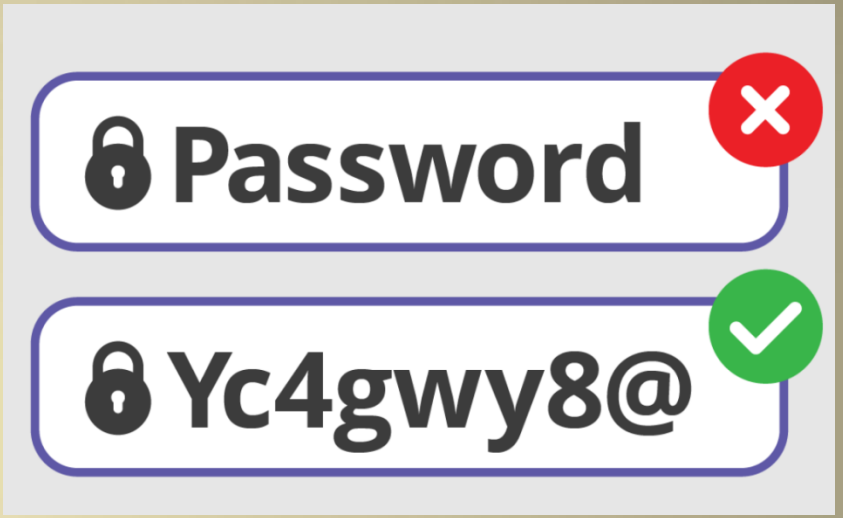
➢ **Passkeys are safer than passwords!**

Password Strength Checker

Free Password Strength Checker:

www.nordpass.com/secure-password/

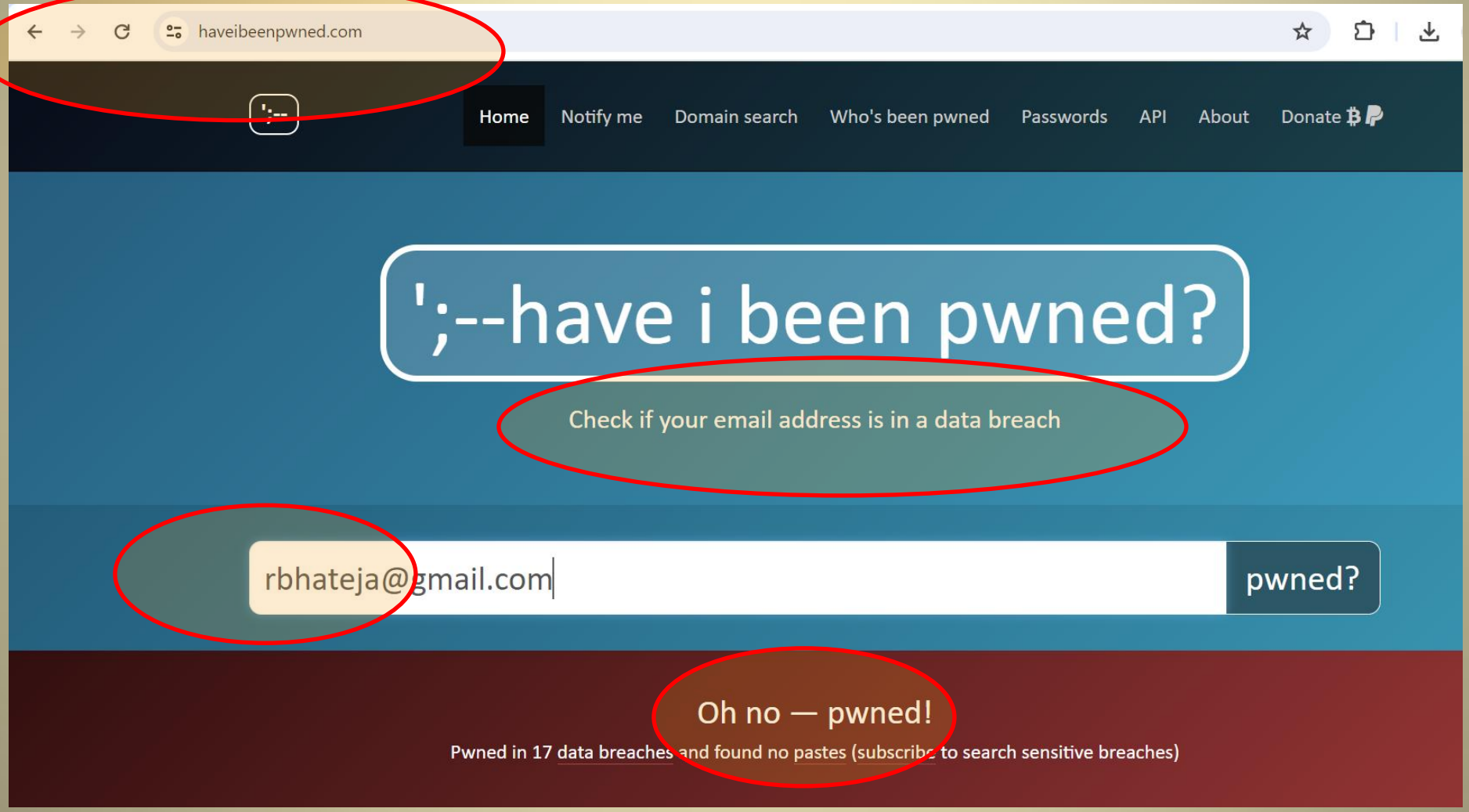




CAUTION:
Generally avoid checking your password with websites unless they’re from a reputed company.
Password managers do this for you automatically.

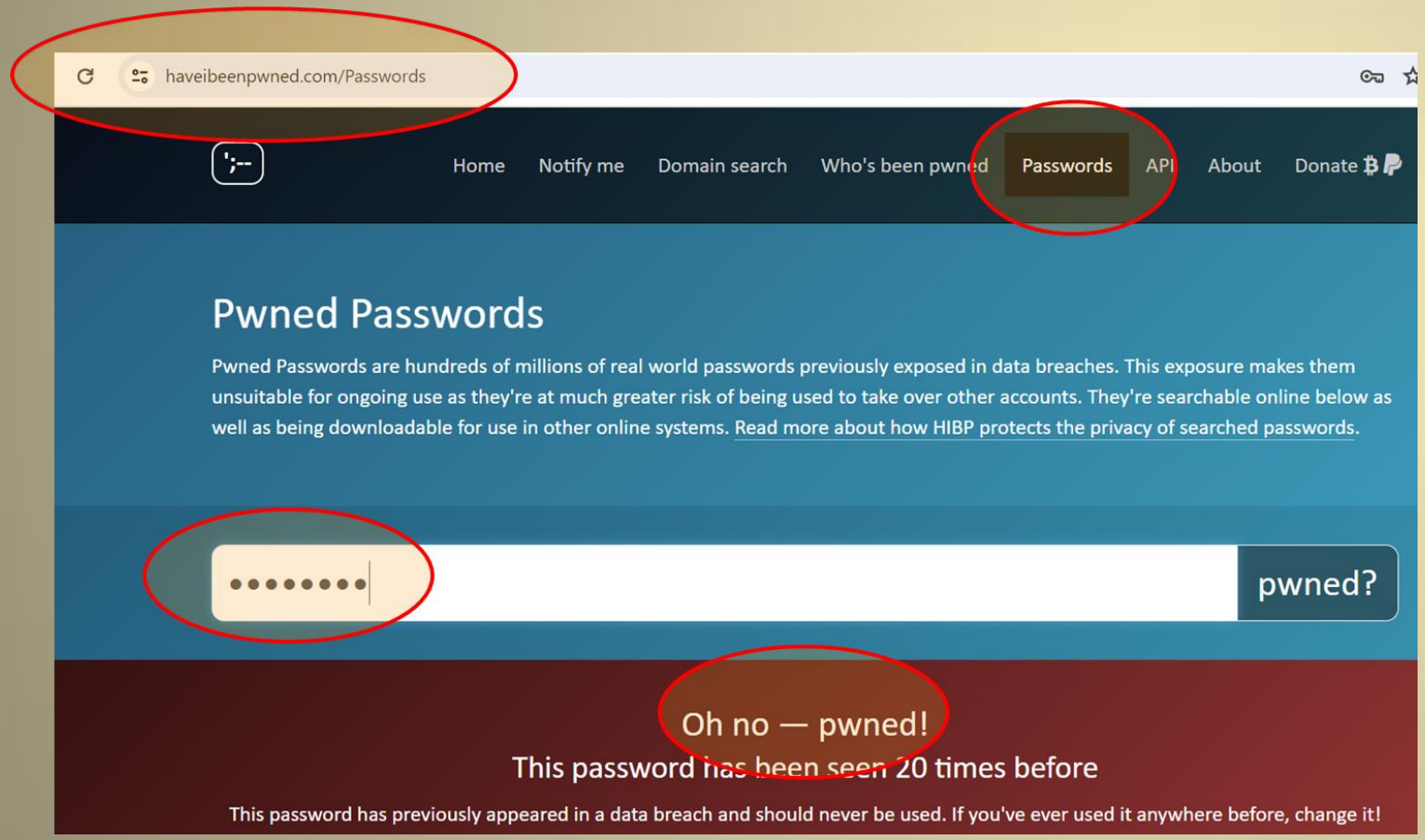
IS YOUR EMAIL IN DATA BREACHES?

https://haveibeenpwned.com



Does your Password Appear in Data Breaches?

https://haveibeenpwned.com



Weak Links

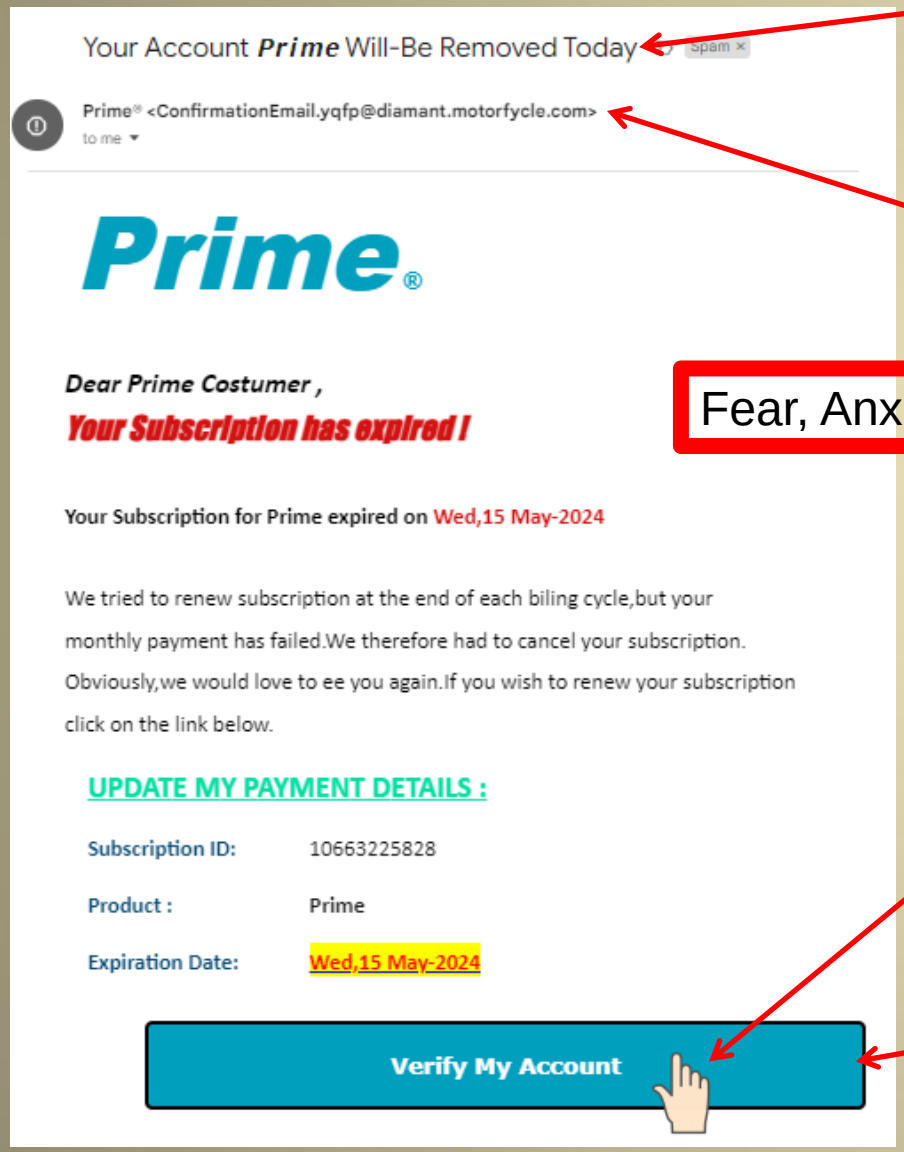
Unauthorized access to your computer, phone or email can lead to severe consequences.
These are major weak links.

Make sure you **PROTECT**:

- Computers
  - Be very careful about where you're downloading software from
  - Don't give anyone access to your computers – in-person or remotely
- Phones
  - Protect your phone with a SIM PIN (aka "number transfer PIN")
  - Robust screen lock (Fingerprint / PIN / Pattern) – avoid facial recognition
  - Fast auto-lock timeout to lock screen
- Email and critical accounts
  - Use MFA
  - Use a hardware key (like Yubikey) for extra security
    - Requires physical key (and optionally a PIN)


Identifying and Avoiding Scams

How to Spot Fake Emails



Float cursor over button to display link

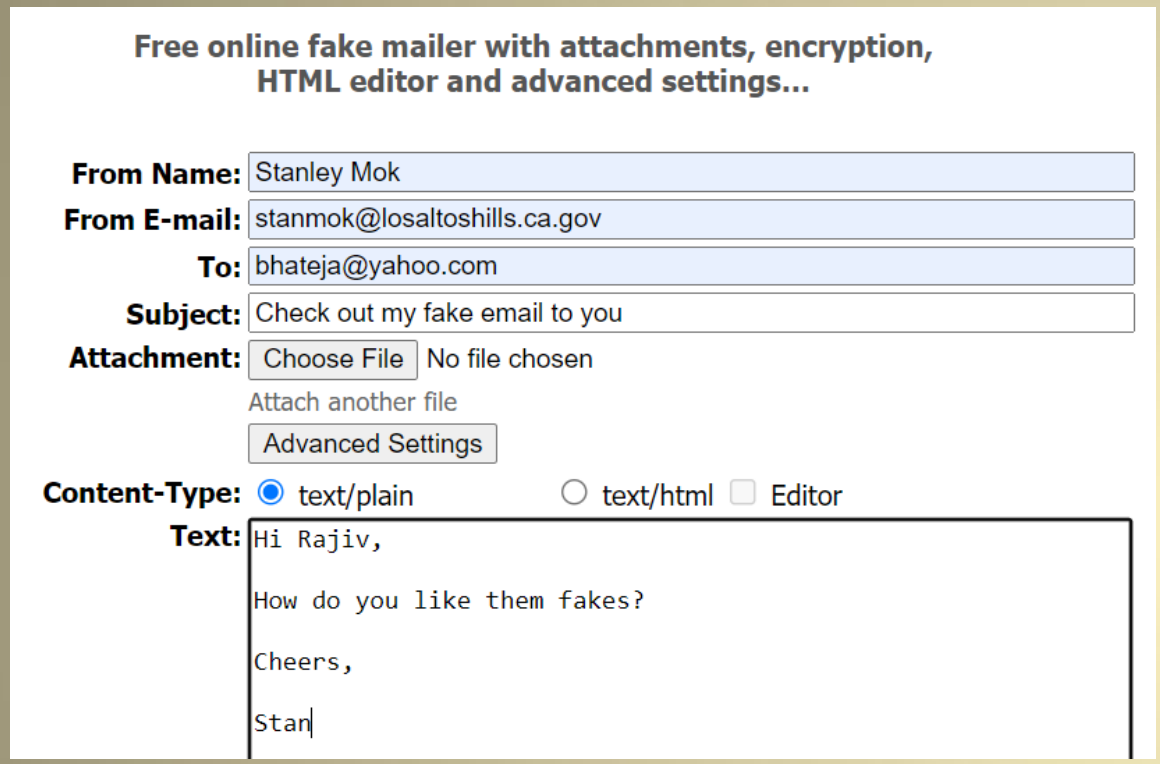
Prime® <ConfirmationEmail.yqfp@diamant.motorfycle.com>
to me

Fear, Anxiety, Urgency

Float cursor over button to display link

https://www.amazon-prime-renew.com – FAKE!!

How Easy is to Fake an Email?



Yahoo mail sent it to spam.
Gmail did not allow it go through at all.

Not all email providers are going to catch all fakes.

Solution: Confirm by other means if suspicious.

To: bhateja@yahoo.com
Subject: Check out my fake email to you
From: "Stanley Mok" <stanmok@losaltoshills.ca.gov>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: stanmok@losaltoshills.ca.gov
Reply-To: stanmok@losaltoshills.ca.gov
Content-Type: text/plain; charset=utf-8
Message-Id: 20240612223911.0A2AD1D7C@emkei.cz
Date: Thu, 13 Jun 2024 00:39:11 +0200 (CEST)
Content-Length: 54

Hi Rajiv,

How do you like them fakes?

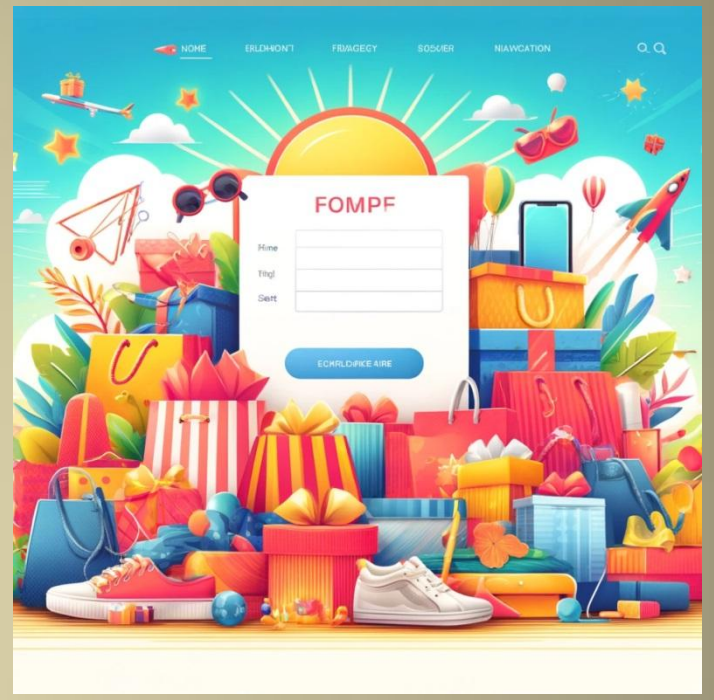
Cheers,

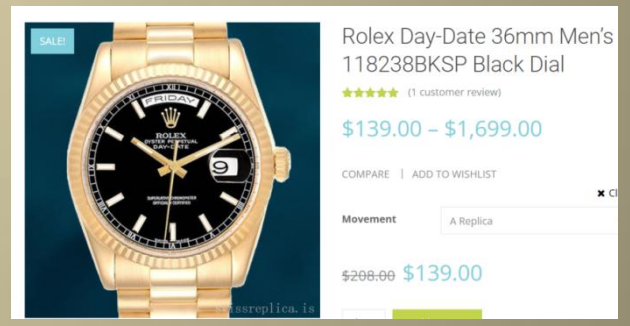
Stan

Marketplace Fraud

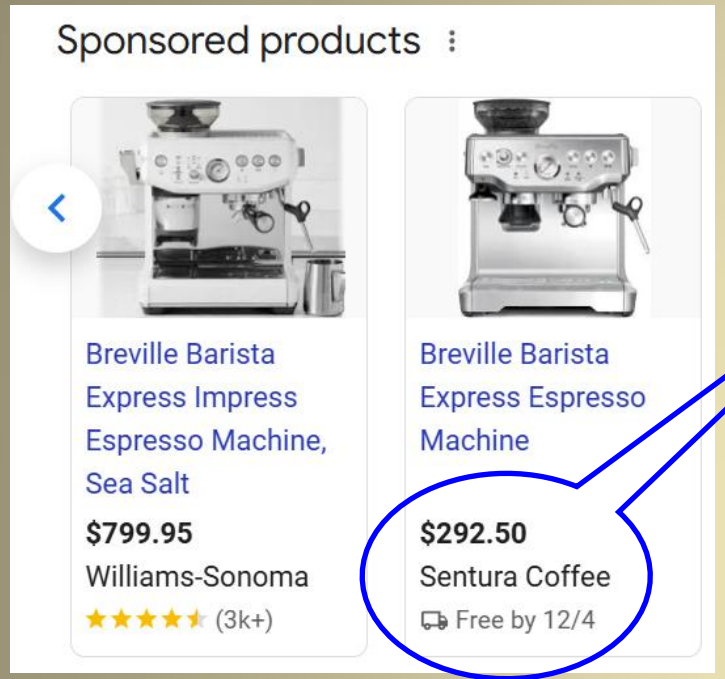
- Account hijacking
  - Solution: Protect your credentials, use Multi-Factor Authentication
- Phishing for identify info
  - Solution: Don't share your DOB, SSN, etc. with marketplaces

    [But be aware: that info could be out there already]
- Delivery redirection
  - Solution: Watch out for email notifications of address/phone number change
- Inaccurate/misleading listing / Too good to be true
  - Solution: READ CAREFULLY. Only use well-reputed sites
- Use trusted sites and payment methods
  - Solution: Use credit cards or **protected payment methods**
    - **Not Western Union, Giftcards, Zelle, etc.**
  - Stay within a protected marketplace
    - AirBnB host suggests offline transaction **DECLINE**



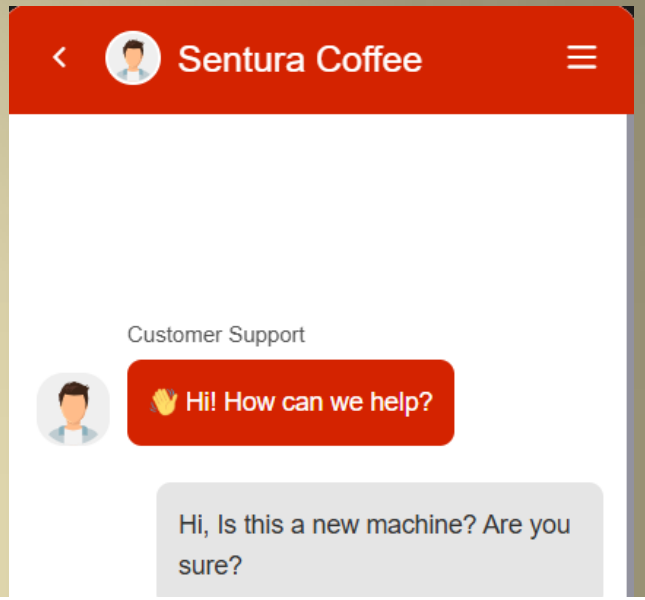


Search: Breville Barista Express Espresso Machine



Typically around $700-$800

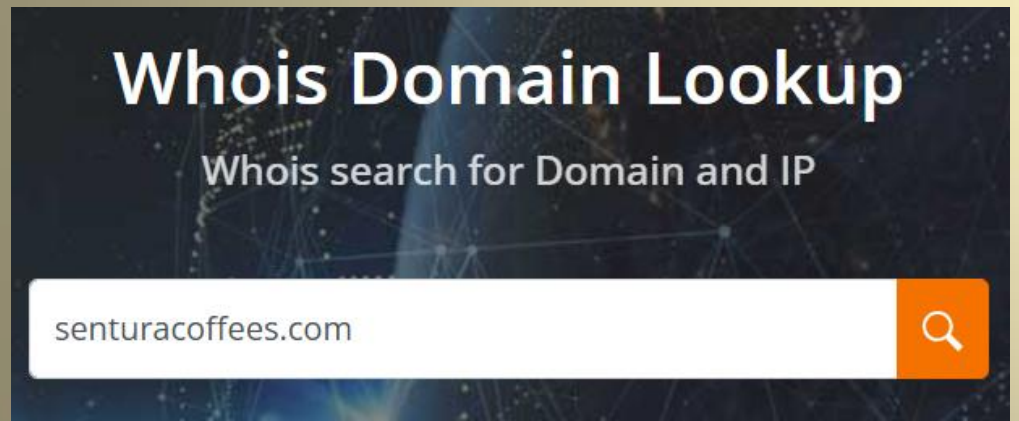
WOW! GREAT DEAL!!!

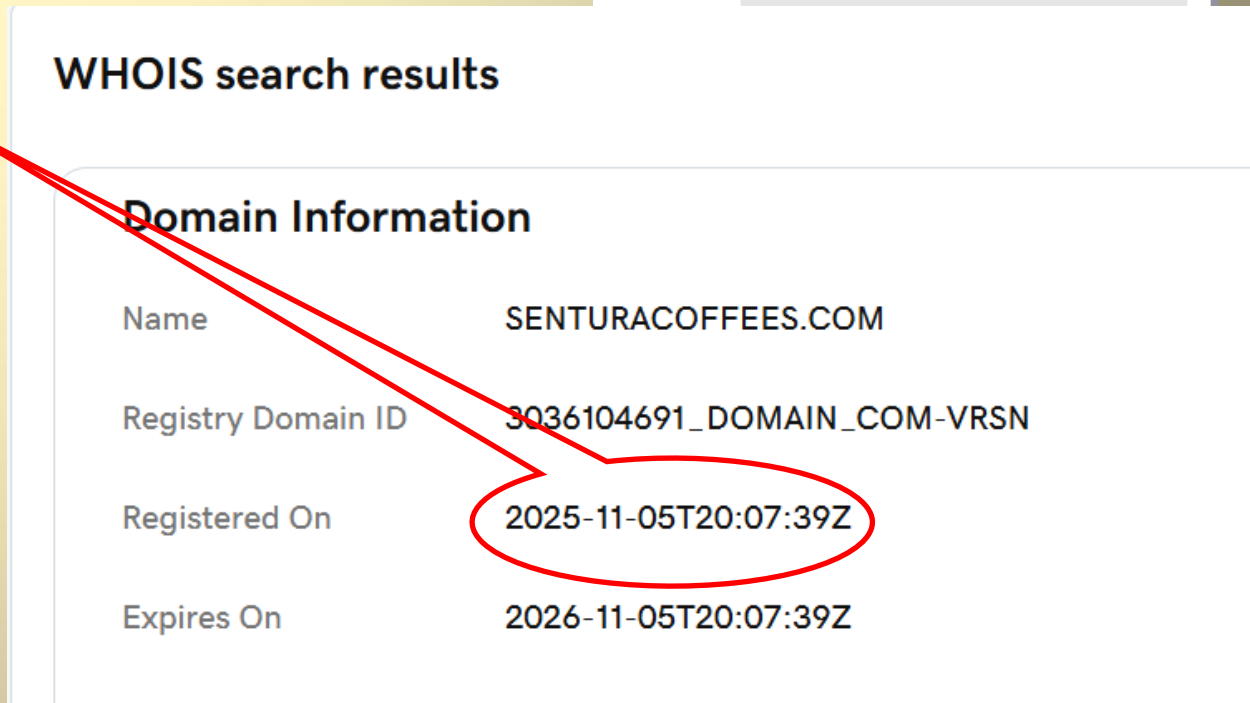


WHOA!
Very new website!!

Likely scam.

WHOIS.COM lookup

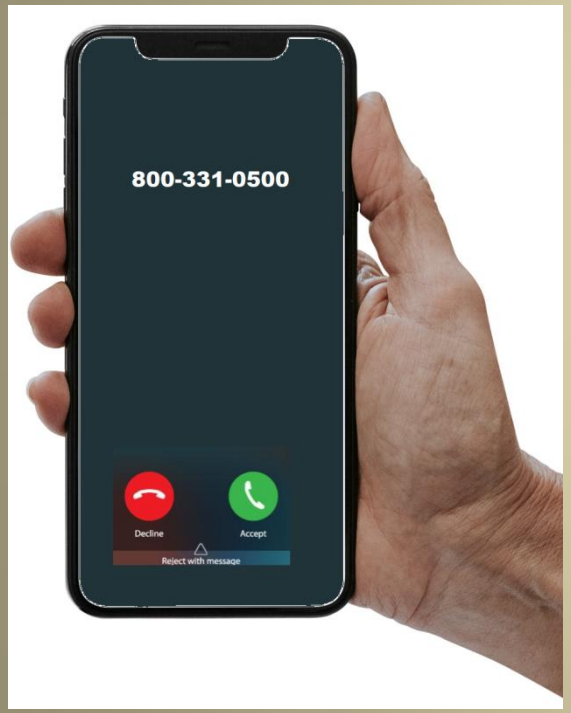




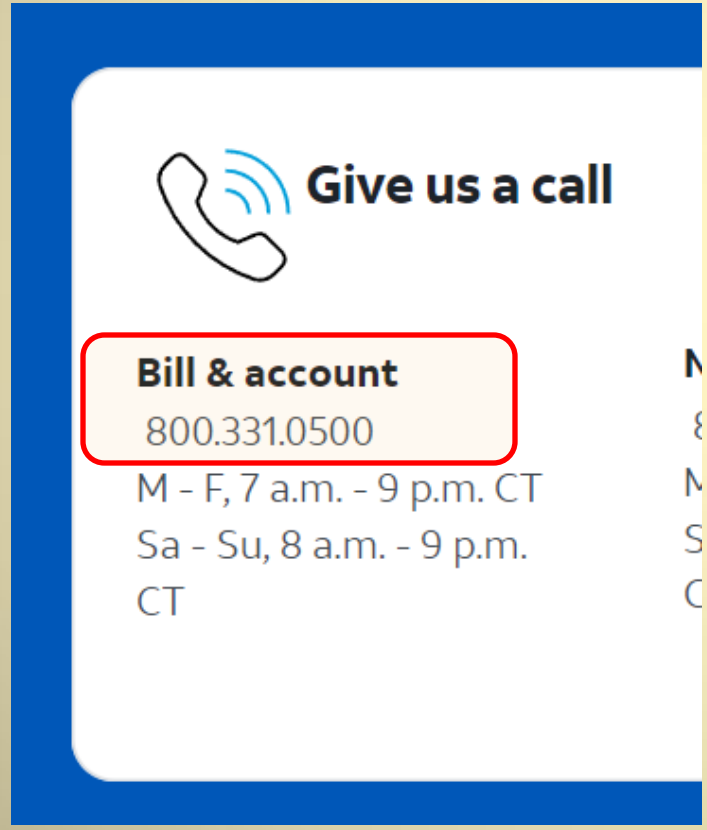
Example of a Phone Scam

Call from AT&T

Free iPhones !!!



Check AT&T website:
Number checks out!!
Looks legit…



3 weeks later…

No iPhones

Account is hacked

It's a SCAM!

But HOW ??

BUT…

I VERIFIED THE PHONE NUMBER!!

IT WAS AT&T.

Q, HOW DID THIS HAPPEN?

A. The scammer called YOU.
They spoofed the AT&T phone number.

GOLDEN RULE: When in doubt…

RULE:

1. “Don’t call me. I’ll call you.”

2. “Let me call back at the verified number.”

SIM Swapping

CAUTION:
If you share your confidential information with a scammer, banks may not reimburse you.

SIM Swapping: one of the most pernicious of all scams

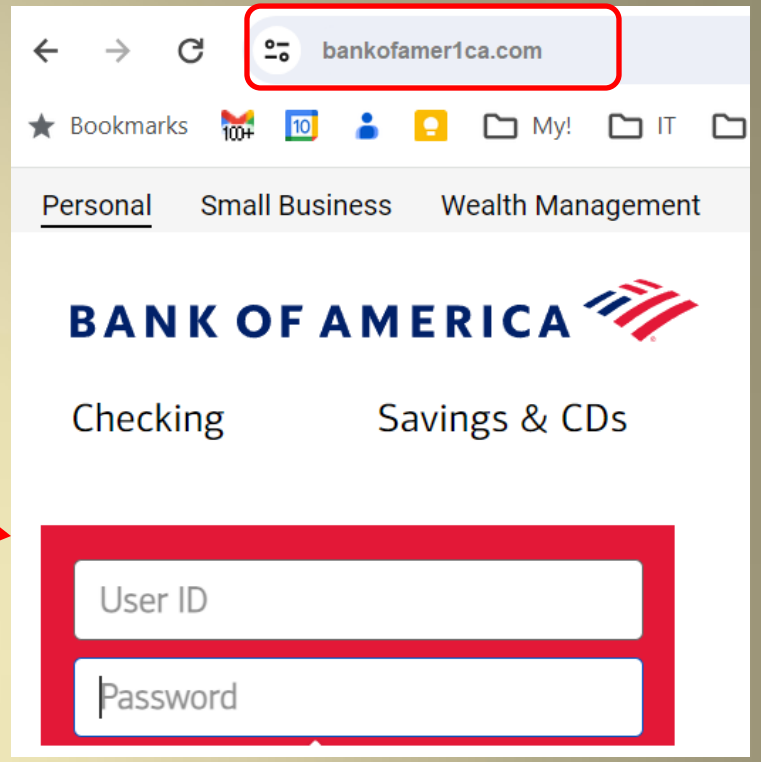
- Lose access to your phone number
- Scammer can reset your passwords over email
- Scammer can intercept text one time passwords
- Two factor authentication is useless

How To Prevent SIM Swapping

- Add a **"number porting" PIN** to your cellular service provider account
- Be super attentive to **emails and texts from your cellular service provider**
- Use **authenticator apps** whenever possible
- **Never share codes** for two-factor authentication with anyone

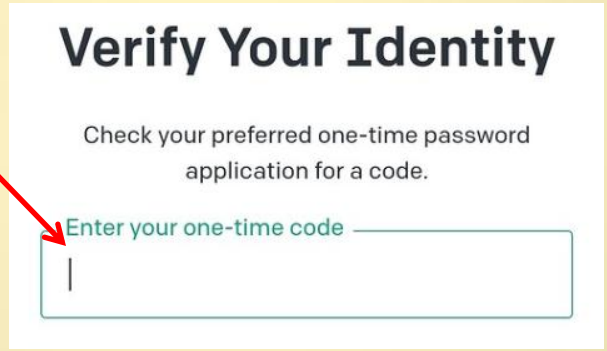
Man in the Middle Attack

Step 1: Scammer tricks you into thinking you're on a bank site: bankofamer1ca.com (replace i with 1). **Scammer can see what you enter on this site.**



Step 2: You enter your username and password.
Scammer enters your credentials on the REAL BofA site

Step 3: BofA texts you a **one time code** or you enter code from **your authenticator app.**



You enter the code on the **fake BofA web page**

Scammer now has your one time code.

Step 4: Scammer enters your code and gets into your account.

SOLUTION: Make sure you're on the right website.

Avoiding Man in the Middle Attack

RULE:

Make sure you're on the real website.
Don't click on a link in an email or text.
Go to your bookmarked link or type it in yourself.

Protecting Accounts and Devices

Protect Your Phone

Face ID unlock has inherent weaknesses

- Can be faked with AI
- Phone can quickly be held up to your face and unlocked

- **Recommend: Use a fingerprint, PIN or pattern (rather than facial recognition) to unlock your phone**

Public WiFi / Hotspots

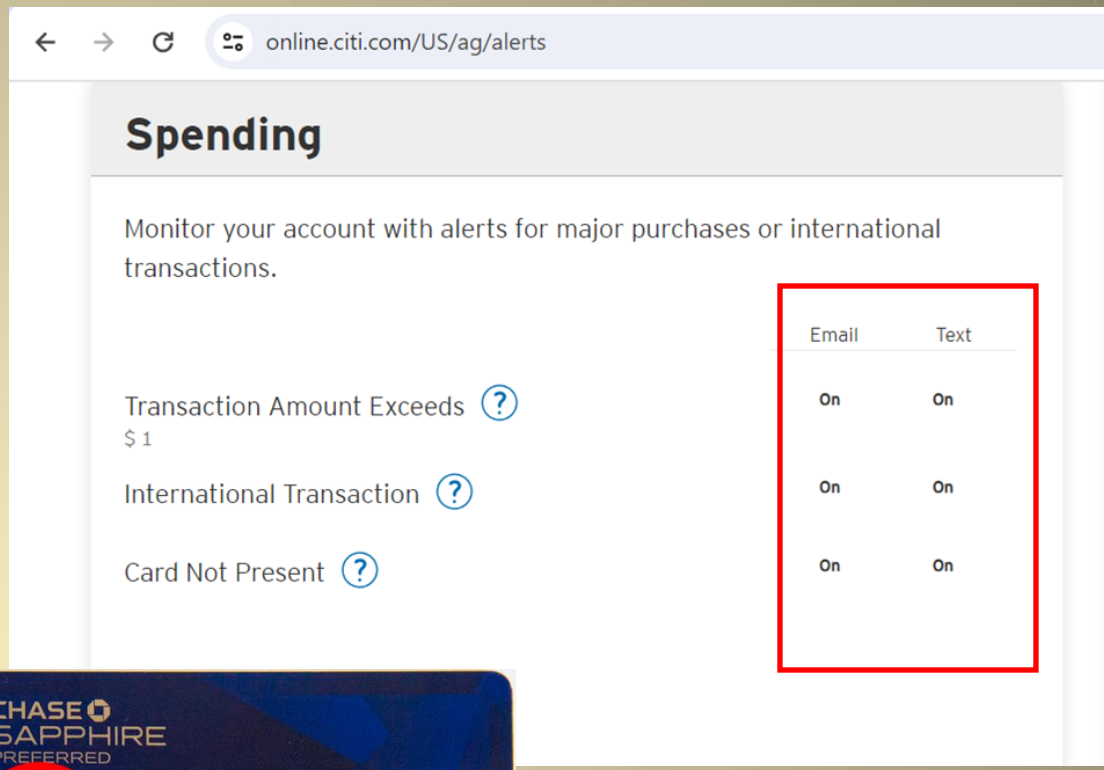
- Using a public WiFi or hotspot allows attackers to sneak malicious software (malware) into your device, display infected ads or using a phishing form to steal passwords.

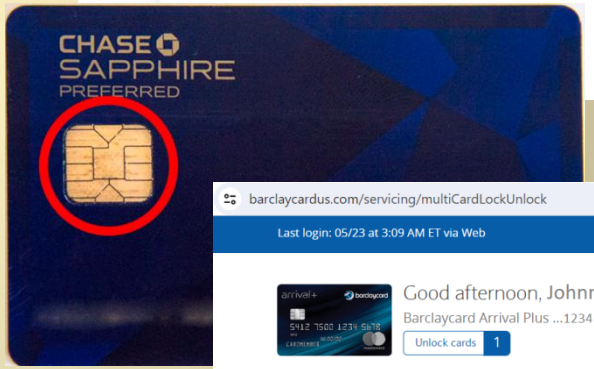
- **Recommend: If using a public WiFi network, use VPN from a reputed vendor to protect your phone from malicious software. Or use mobile data.**

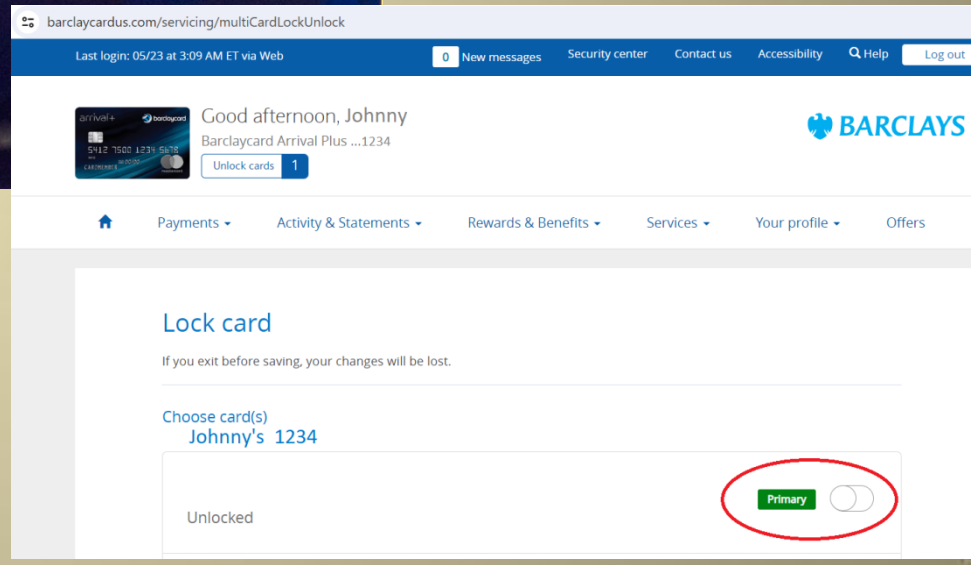
- Some cellular service providers automatically use VPN when using WiFi or hotspots

Protect Credit Card & Financial Accounts

- Use **multi-factor authentication (MFA)**
- **Setup text/email alerts** for your financial accounts
- Bank ATMs are more secure than retail ATMs
- Be careful of devices with skimmers
  - Inspect device before using your card
- Use a **chip reader or tap card.** Avoid swiping!
- Promptly **notify your credit card company** of any unrecognized charges
- If concerned about card security, **LOCK your card**
- Set up **PINs for IRS and FTB** accounts to prevent scammers filing for a refund on your accounts







Credit Freeze – Prevent Others from Opening an Account in Your Name

Please a credit freeze with all three credit reporting agencies:

TransUnion, Equifax, Experian

- Allows your current accounts access to your credit
- **Prevents fraudsters from opening an account in your name**
- Temporarily UnFreeze to open a new account

Credit reporting companies are going to try and sell you credit locks

NOTE: Credit *Freezes* are *Free!*

Credit Locks are not free – and you don't need them

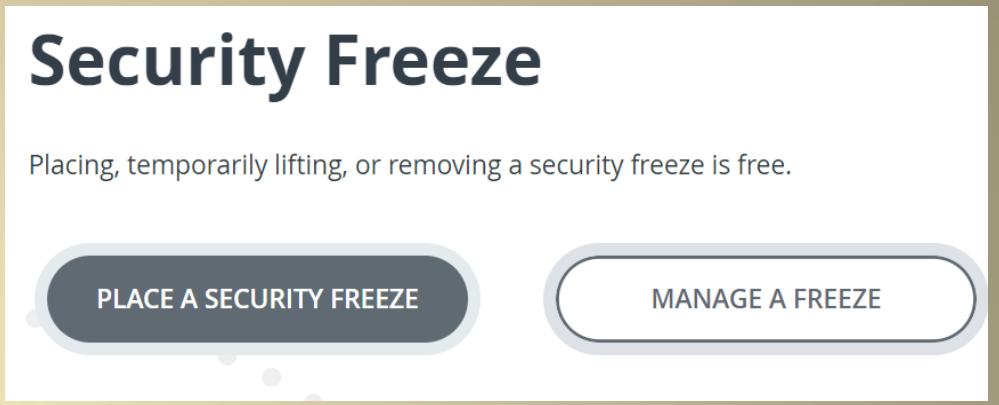
Credit Security Freeze – How To

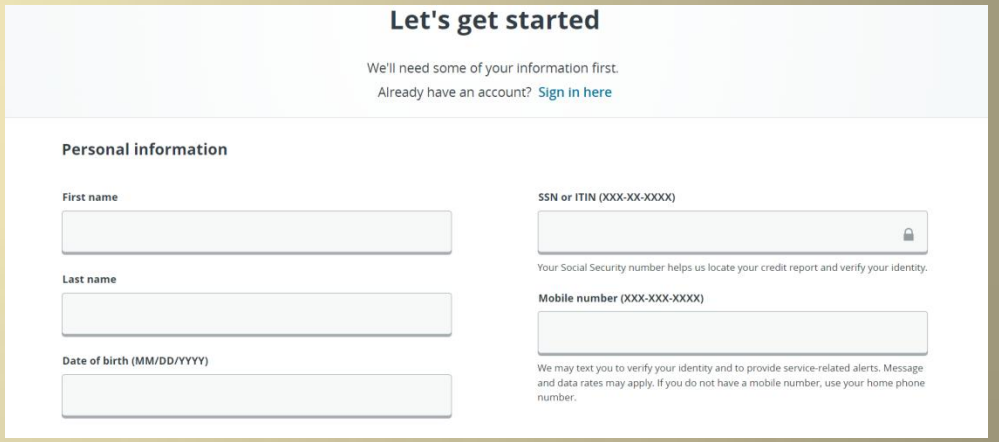
https://www.equifax.com/personal/credit-report-services/credit-freeze/

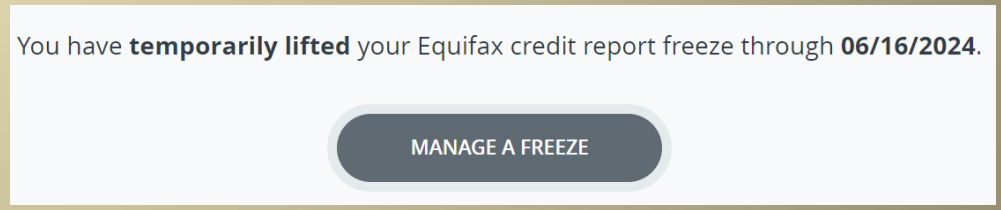
https://www.transunion.com/credit-freeze

https://www.experian.com/freeze/center.html

- FREEZES are FREE. Locks are not. A freeze is all you need.
- A freeze can be permanent (recommended), or temporary.
- You can temporarily LIFT a freeze if/when you apply for an account
  - Lift can be scheduled to last for 1-30 days
  - Freeze automatically reinstated after the temporary lift







Recommendations and Additional Resources

Summary of Recommendations

- Never re-use passwords.
  - Use a **password manager**
  - Use **Multi-Factor Authentication** and/or a **hardware key** to secure key accounts
    - Authenticator app is safer than one-time PIN
  - **NEVER share a one-time PIN with anyone else**
- Protect against SIM Swapping
  - **Add a "number transfer PIN"** or other credential to your cellular service provider account
- **Set up and monitor alerts** from your bank, credit card company, cell provider, brokerage
- **Avoid clicking on links** in emails/texts
- Protect your phone: **robust screen lock**
- **"Don't call me, I'll call you"** – phone numbers can be hacked
- **Place a credit freeze** with all three credit reporting agencies
- **Be wary of acting in haste** in response to an unverified call or text

More Good Practices

- Use VPN when using public WiFi
- Avoid clicking on links in your email or text messages – convenient but could take you to an imitation website
  - If you do click on a link, check the web address (URL)
- Avoid calling an 800 number listed in your email or text messages.
  - If you do, check to make sure the number is listed on the organization's website
  - Alternatively, call the organization's regular phone number (from their website)
- Do NOT use public charging cords or chargers. These chargers can be compromised.
  - Use your own charging adapter.
- Be aware of messages from your cell phone service provider ("SIM swapping")
  - https://www.businessinsider.com/credit-card-phone-theft-sim-swap-identity-theft-investigation-2023-4
- Don't leave your AirDrop (iOS) or Nearby Share (Android) enabled

SIM Protection Setup: Cell Carrier Links

AT&T: https://www.att.com/support/article/wireless/000102016/

Verizon: https://www.verizon.com/support/knowledge-base-309294/

T-Mobile: https://www.t-mobile.com/support/plans-features/help-with-t-mobile-account-fraud#pin

US Cellular: https://www.uscellular.com/support/faq/myaccount (Account Lock)

IF YOU ARE A VICTIM

- If you believe you are a victim of a Cybercrime, you should take the following steps:
  - Gather information
  - Report the incident
  - Change passwords
  - Contact your financial institution(s)
  - Report the incident to your local police: Santa Clara County Sheriff
  - FTC at reportfraud.ftc.gov
  - Call the AARP Fraud Watch Network Helpline 877-908-3360
  - Spread the word about fraud

Additional Articles

- The Day I Put $50,000 in a Shoe Box and Handed It to a Stranger
  - **https://www.thecut.com/article/amazon-scam-call-ftc-arrest-warrants.html**
- My phone, my credit card, my hacker, and me
  - **https://www.businessinsider.com/credit-card-phone-theft-sim-swap-identity-theft-investigation-2023-4**
- A former White House scientist was scammed out of $655,000. Then came the IRS.
  - **https://www.washingtonpost.com/dc-md-va/2023/12/14/cyber-crime-scams-irs-taxes/**
- Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’
  - **https://www.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html**
- ‘I had fun’: Alleged scammer takes credit for Graceland foreclosure upheaval
  - **https://www.latimes.com/entertainment-arts/story/2024-05-29/nigerian-scammer-graceland-sale#**
- Fake Obama created using AI video tool - BBC News
  - **https://www.youtube.com/watch?v=AmUC4m6w1wo**


THANK YOU

QUESTIONS?

BACKUP SLIDES

Clinic Topics

- Username/Password security checks: www.haveibeenpwned.com
- Password strength checks: www.nordpass/secure-password
- Setting up a password manager
- Credit card text/email alerts
- Multifactor authentication
- Hardware key
- Credit freezes
- SIM swapping prevention (set up PIN with cellular service provider)
- Credit card lock capability
- Inactive account manager