

# **CYBERSECURITY AVOIDING SCAMS STAYING SAFE ONLINE**

**LOS ALTOS HILLS TECHNOLOGY COMMITTEE**

**STAN MOK (COUNCIL LIAISON)  
RAJIV BHATEJA (CHAIR)  
AMEESH DIVATIA (VICE CHAIR)  
RON HALEY**

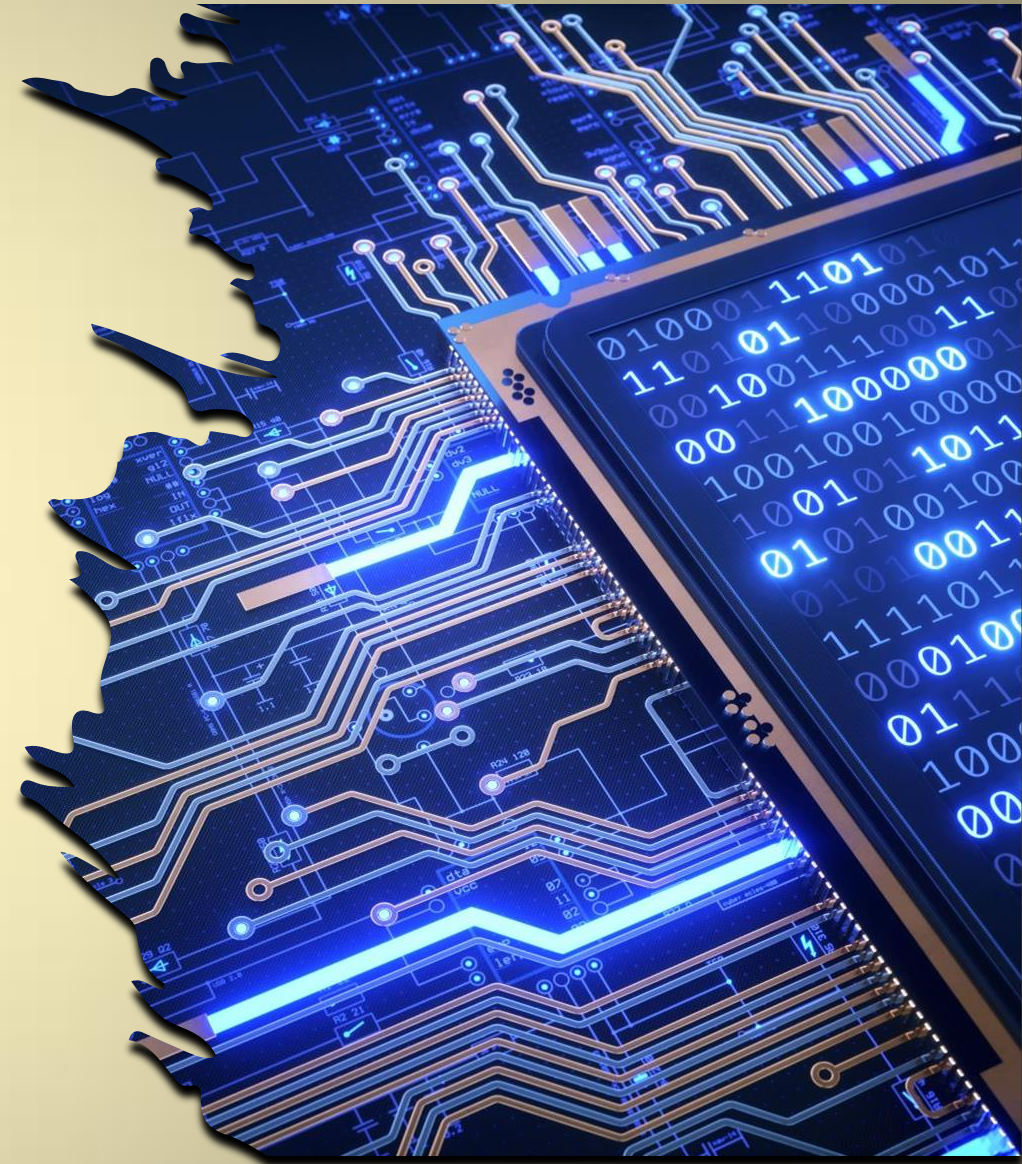
**LEW JAMISON  
ANNIE JU  
GEORGE LEE  
JOHN SWAN**

**JUNE 23, 2024**



# Agenda

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







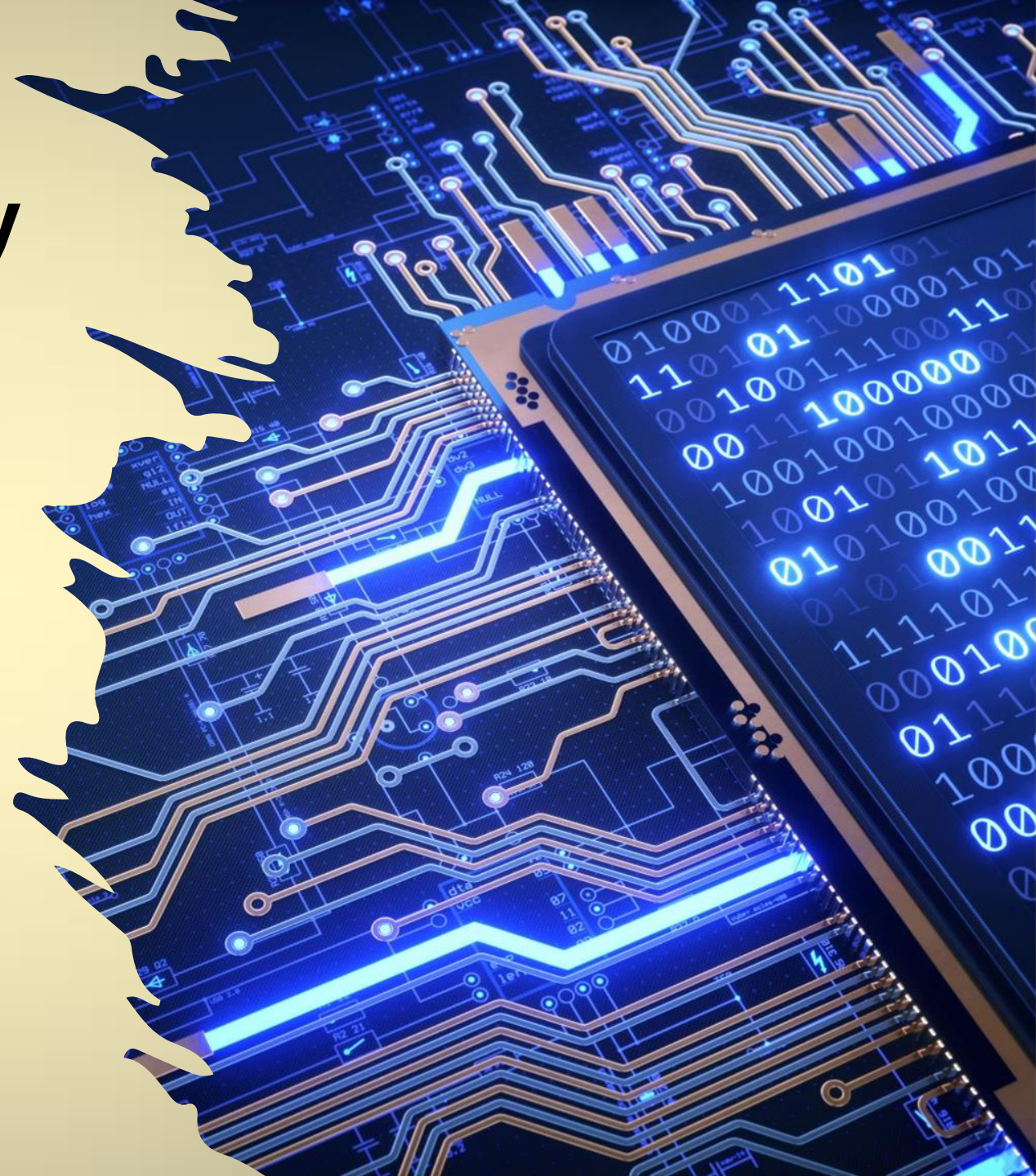
# **Introduction to Cybersecurity and Scams**



# What is Cybersecurity

The term 'cybersecurity' refers to the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative.

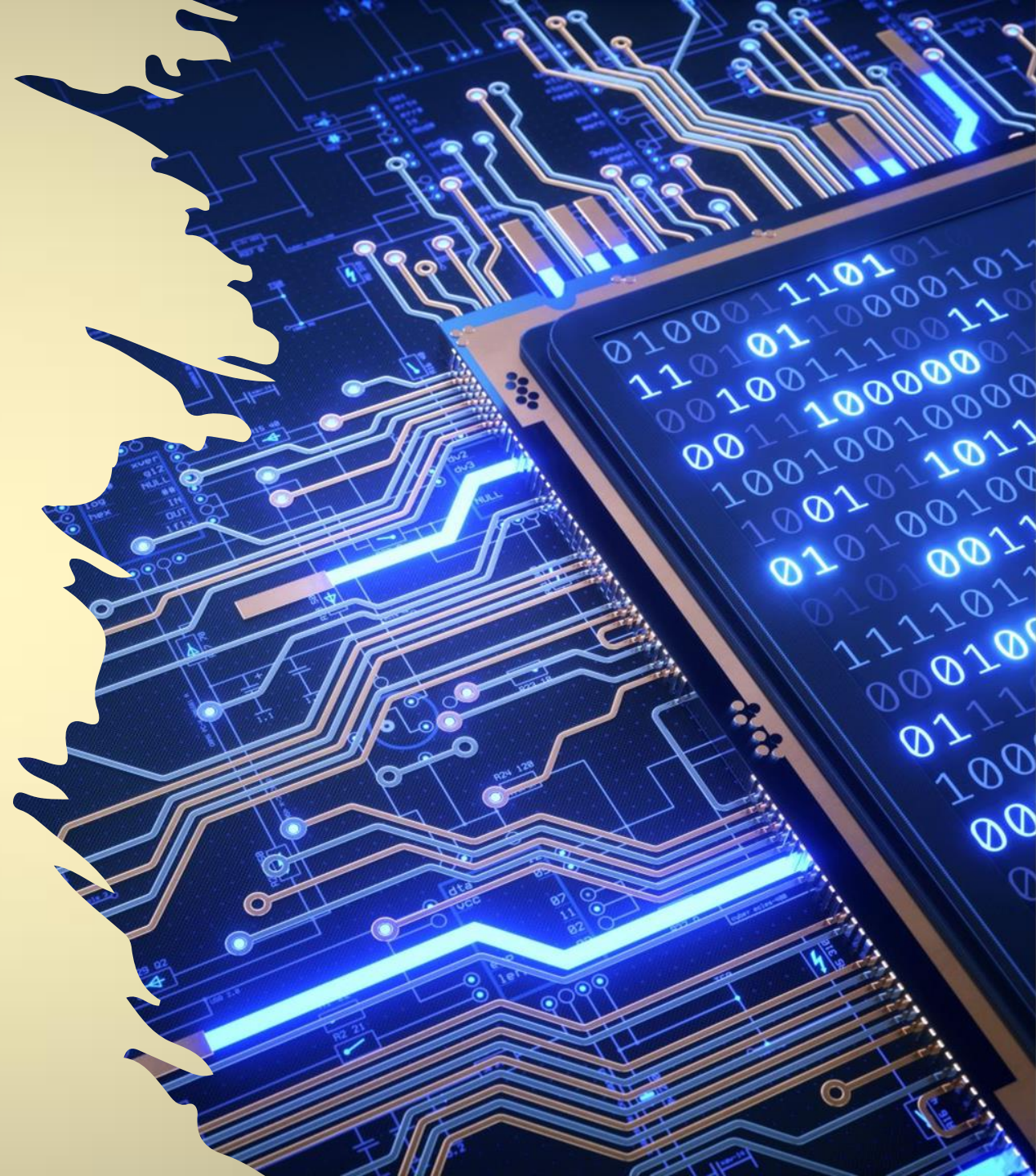




# What are Scams

Scams, often referred to in the context of cybersecurity, involve deceptive practices that aim to manipulate individuals into divulging confidential information, transferring money, or granting access to their systems.

Scams can take various forms, such as phishing emails, fake marketplaces, or advance payment frauds, and are designed to exploit the victims for financial gain or to disrupt normal business processes.





# 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





The image features a detailed, high-tech circuit board as a background. The board is populated with various electronic components, including integrated circuits, capacitors, and resistors, all interconnected by a complex network of fine, glowing lines. A prominent feature is a large, rectangular area on the right side of the board, which is filled with glowing binary code (0s and 1s) in a light blue or cyan color. The overall aesthetic is futuristic and digital, with a color palette dominated by dark blues, greys, and vibrant, glowing yellows and oranges. The text "Be Informed" is centered over the image in a large, bold, black font.

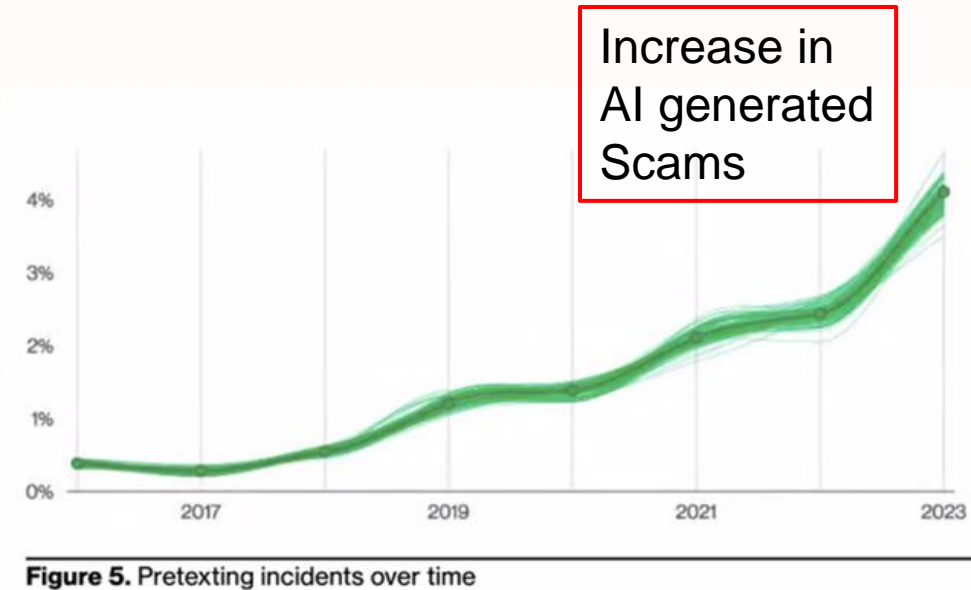
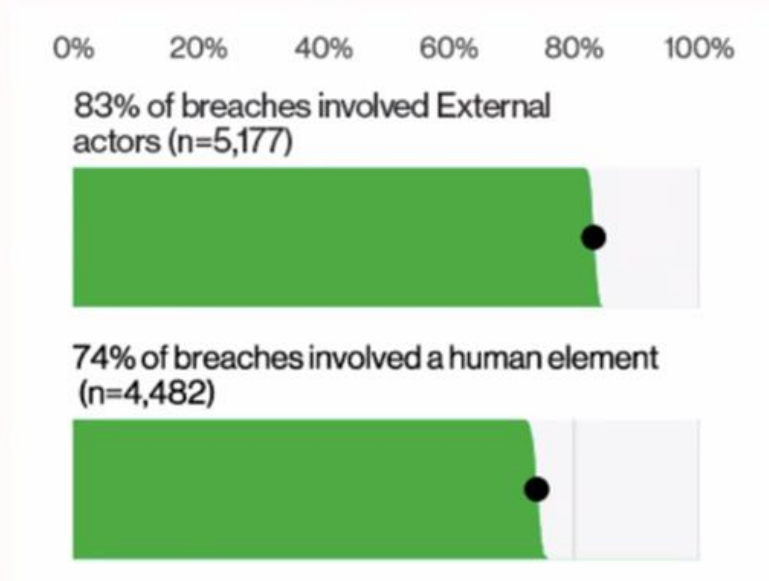
**Be Informed**



# Growth of Scams



## Year in Review



**DBIR 2023 (Verizon)**  
2023 Data Breach Investigations Report

\_\_\_\_\_ is investigating *whether* a large trove of customer data was stolen from the company *after* information about the firm's clients was *offered for sale* on a cybercrime forum earlier this week.

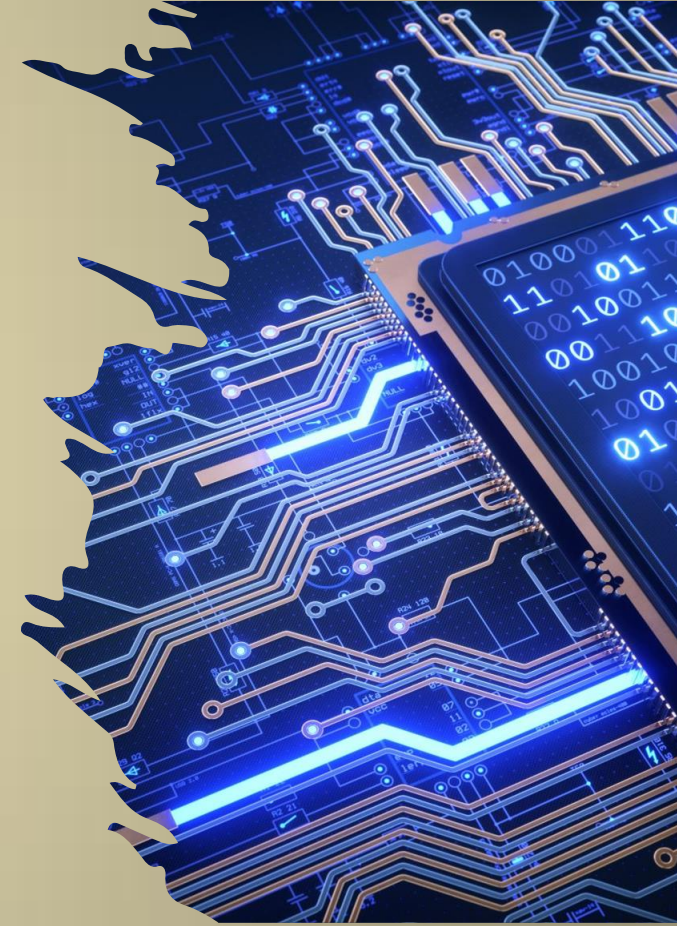
**October 2023**

**Attack: "Credential Stuffing"**



# Common Types of Scams

- Government agency (pretending to be: IRS, Customs, USPS...)
  - Example: <https://www.irs.gov/newsroom/tax-scamsconsumer-alerts>
- Corporations (pretending to be: UPS, Wal-Mart, Amazon, EBay, PayPal, AT&T, banks...)
  - Example: <https://corporate.walmart.com/privacy-security/fraud-alerts>
- Call Centers / Technical Assistance (pretending to be: Microsoft, Norton, McAfee...)
  - Example: <https://bit.ly/microsoft-scams>
- Financial
  - Example: credit card cloning/skimming, phone hacking, email phishing
- Romance
  - Search for “social catfish” on YouTube
- Family, friends, caregivers
  - Example: <https://www.plano.gov/2125/Parent-Scam>
- Stolen / re-written paper checks
  - “You can buy checks on the internet for \$45, with a perfectly good signature. There is one website that offers a money-back guarantee. It’s like Nordstrom.”
    - John Ravita, Director of Business Development, SQN Banking Systems





# Scammer Tactics

- AI-Powered Scams
- Phone Scams
- Text Scams
- Email Scams
- Student Loan Forgiveness Scams
- Creating a Sense of URGENCY, FEAR
- Building Rapport with Casual Talk
- Catching you at a busy time when you're distracted (soccer field, traveling, meeting, etc.): you make a hasty decision.

It's important to be aware of these tactics and to be cautious when dealing with unsolicited calls, emails, or messages.

If something seems too good to be true, it probably is.







# **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 Process

**1. Use UNIQUE passwords.**

Never re-use important passwords

**2. Use LONG passwords.**

Use a password manager to generate strong passwords

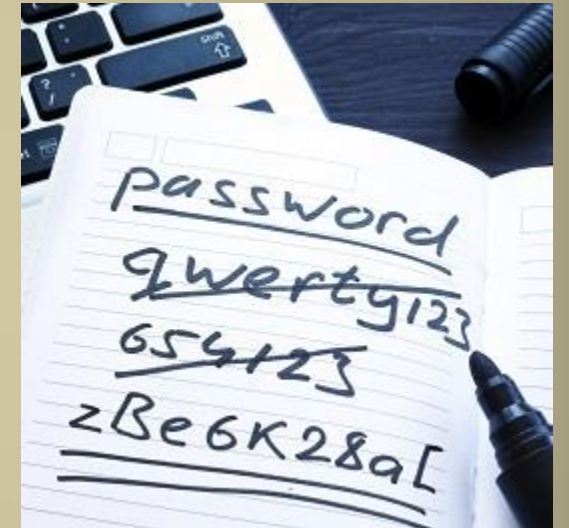
**3. Use MFA where available.**

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

**4. Have I been Pwned?**

Is your password compromised?

**New trend: Passkey**





# What is a Passkey? – Emerging Trend

- A passkey is a **digital token stored on your device** (usually your phone or computer)
  - Similar to GPG technology (private and public key encryption)
- “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...**





# Never Reuse Passwords

“How can I remember all those passwords?”

**Password Manager**





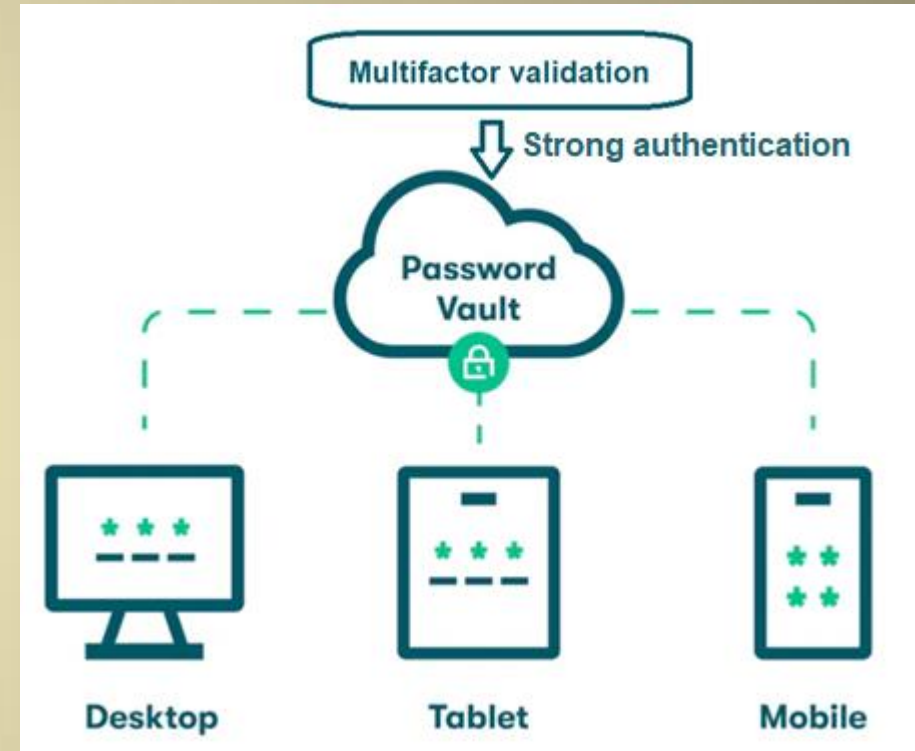
# Password Managers

Independent Password Managers (in no particular order):

- NordPass
- IPassword
- Dashlane
- Keeper
- Bitwarden
- LastPass
- KeePass (actually a “password safe”)

Browser-based password managers: **“Remember this password?”**

- Google Chrome
- Microsoft Edge
- Apple Safari



Password managers **ensure that** you really are at the **correct website** before entering your credentials.

Example: Your Yahoo credentials won't mistakenly be used at Yah00.com

Password managers also advise you if your **password has been hacked** or is not secure.

Password managers also suggest very **strong passwords**.

# Why You Should Use a Password Manager

**Smart Guessing  
Algorithm Cracks 87  
Million Passwords In  
Under 60 Seconds**

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



# Password Strength Checker


Free Password Strength Checker:

[www.nordpass.com/secure-password/](https://www.nordpass.com/secure-password/)

**How secure is my password?**

Take a moment to check if your passwords are easy pickings for bad actors.

.....





Password strength:  **STRONG**

Time it takes to crack your password: **4 months**

---


**Password composition**

Make sure that your password is long enough and contains various types of characters.

- At least 12 characters
-  Lowercase
-  Uppercase
-  Symbols (?#@...)
-  Numbers

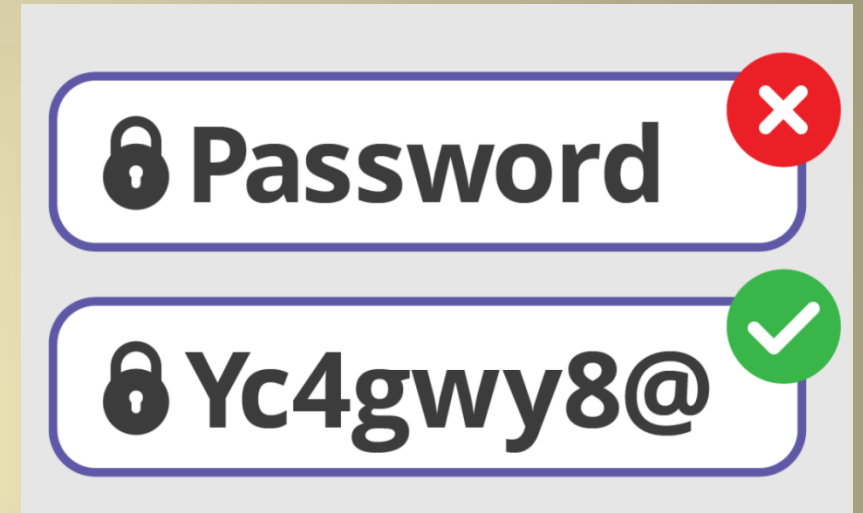
---

Has this password been previously exposed in data breaches?

 **No leaks found!**

powered by [haveibeenpwned.com](https://haveibeenpwned.com)

[Learn how to create and securely store strong passwords in NordPass](#)



## 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>

The screenshot shows the Have I Been Pwned website interface. The browser's address bar is highlighted with a red oval, showing the URL 'haveibeenpwned.com'. The website's navigation bar includes links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is '';--have i been pwned?'. Below it is a subheading 'Check if your email address is in a data breach'. A search input field contains the email 'rbhateja@gmail.com' and is highlighted with a red oval. To the right of the input field is a button labeled 'pwned?'. Below the input field, the result is displayed: 'Oh no — pwned!' (highlighted with a red oval) and 'Pwned in 17 data breaches and found no pastes (subscribe to search sensitive breaches)'.

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email address is in a data breach

rbhateja@gmail.com pwned?

Oh no — pwned!

Pwned in 17 data breaches and found no pastes (subscribe to search sensitive breaches)



# Does your Password Appear in Data Breaches?

<https://haveibeenpwned.com>

haveibeenpwned.com/Passwords

Home Notify me Domain search Who's been pwned Passwords API About Donate

## Pwned Passwords

Pwned Passwords are hundreds of millions of real world passwords previously exposed in data breaches. This exposure makes them unsuitable for ongoing use as they're at much greater risk of being used to take over other accounts. They're searchable online below as well as being downloadable for use in other online systems. [Read more about how HIBP protects the privacy of searched passwords.](#)

..... pwned?

**Oh no — pwned!**

This password has been seen 20 times before

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!



This file is licensed under the [Creative Commons Attribution-Share Alike 4.0 International](#) license.  
Attribution: Santeri Viinamäki

# 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)

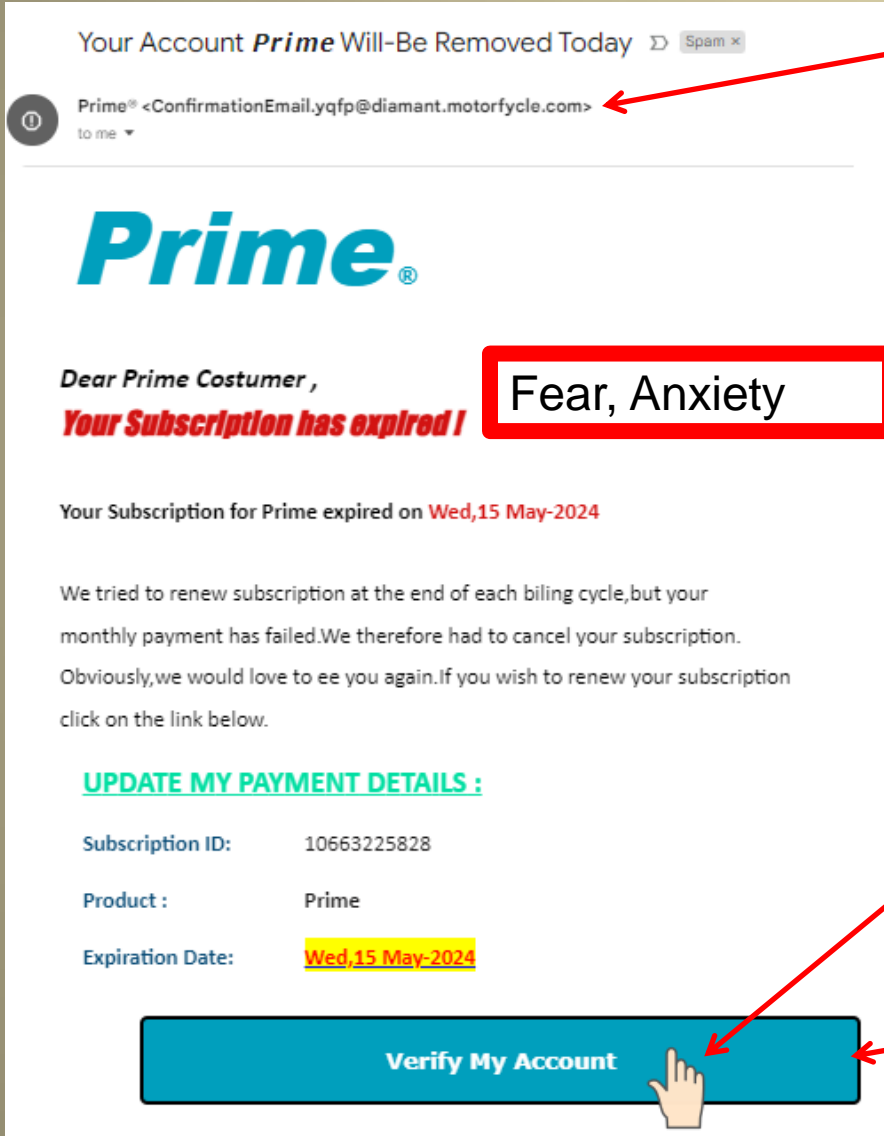






# Identifying and Avoiding Scams

# How to Spot Fake Emails



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

Fear, Anxiety

Float cursor over button to display link

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



# How Easy is to Fake an Email?

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

**From Name:** Stanley Mok

**From E-mail:** stanmok@losaltoshills.ca.gov

**To:** bhateja@yahoo.com

**Subject:** Check out my fake email to you

**Attachment:** Choose File No file chosen  
Attach another file  
Advanced Settings

**Content-Type:** ☒ text/plain ☐ text/html ☐ Editor

**Text:**  
Hi Rajiv,  
  
How do you like them fakes?  
  
Cheers,  
  
Stan

To: [bhateja@yahoo.com](mailto: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](mailto:stanmok@losaltoshills.ca.gov)

Reply-To: [stanmok@losaltoshills.ca.gov](mailto: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

Yahoo mail sent it to spam.

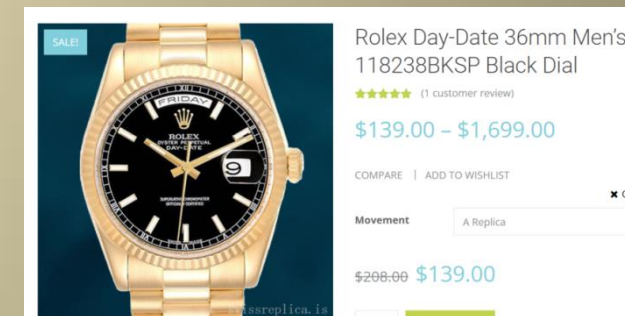
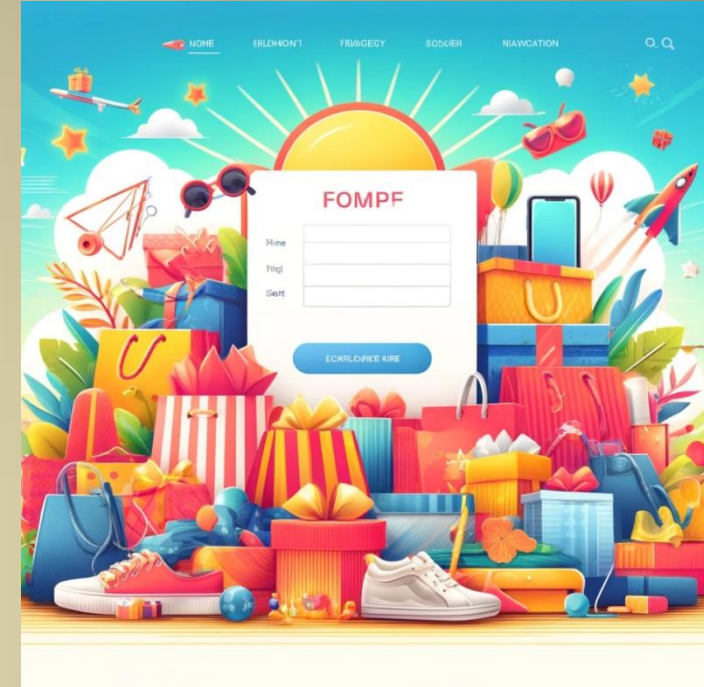
Gmail did not allow it go through at all.

Not all email providers are going to catch all fakes.

Solution: Confirm by other means if suspicious.

# Marketplace Fraud

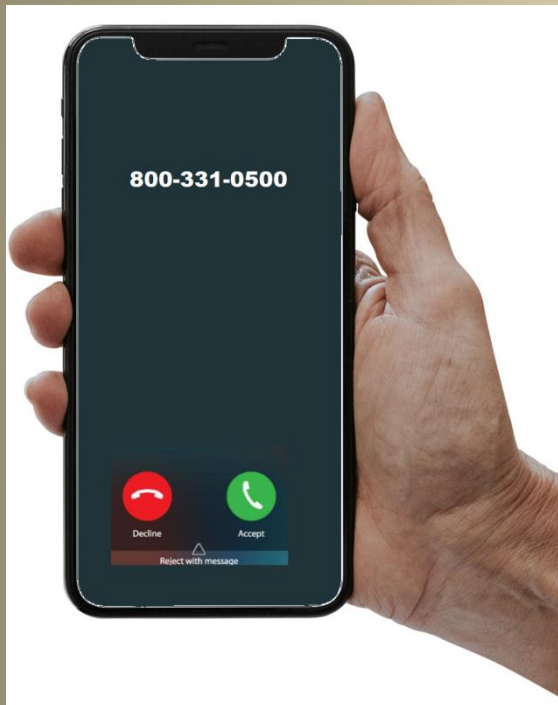
- Account hijacking
  - ❑ Solution: Protect your credentials, use Multi-Factor Authentication
- Phishing for identify info
  - ❑ Solution: Don't share your DOB, SSN, etc. with marketplaces  
[But be aware: that info could be out there already]
- Delivery redirection
  - ❑ Solution: Watch out for email 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**



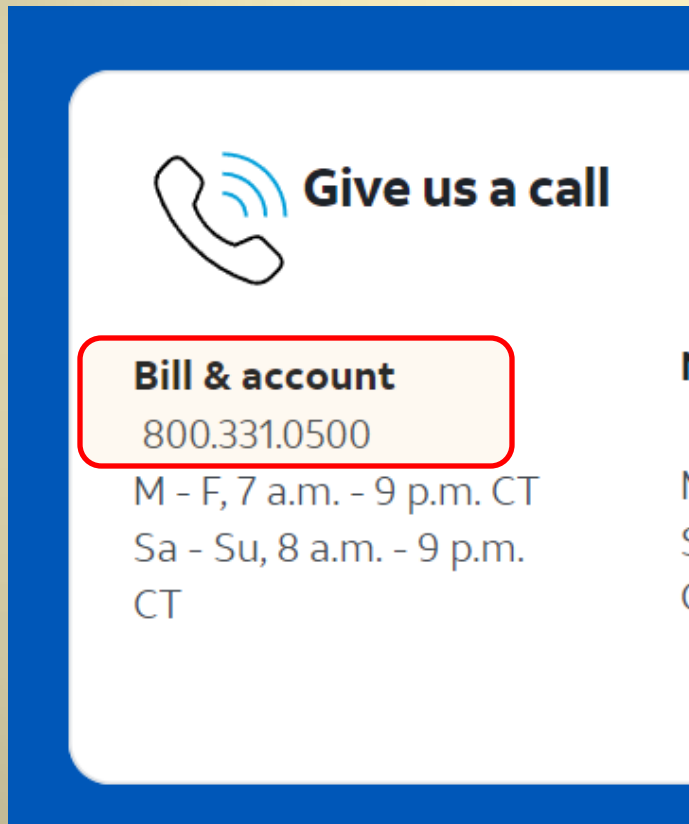


# Example of a Phone Scam

Call from AT&T  
Free iPhones !!!



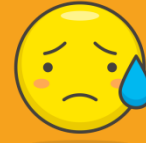
Check AT&T website:  
Number checks out!!



3 weeks later...

No iPhones

Account is  
hacked



It's a SCAM!

But HOW ??

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

**Solution:**  
Tell them you'll call  
THEM at the verified  
AT&T number.

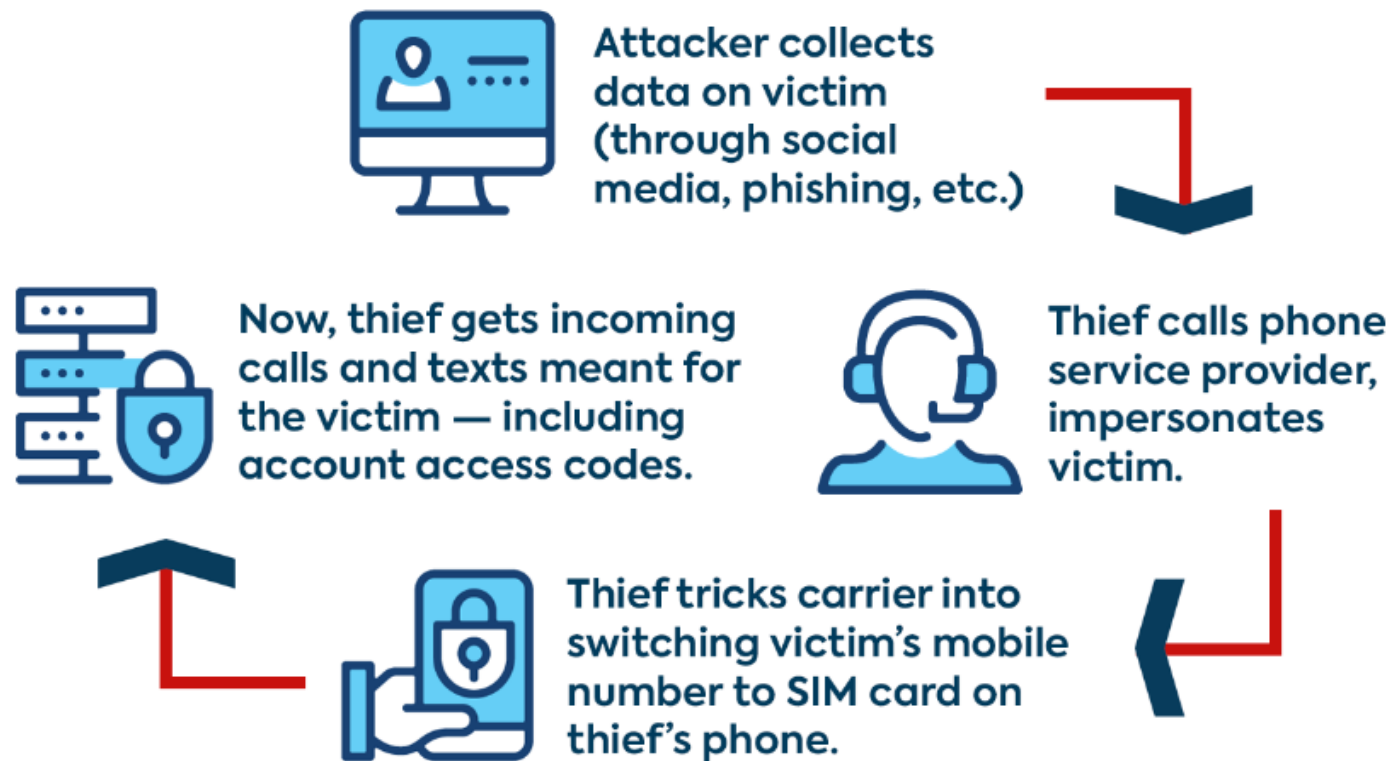
# Avoiding Phone Scams

## **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.

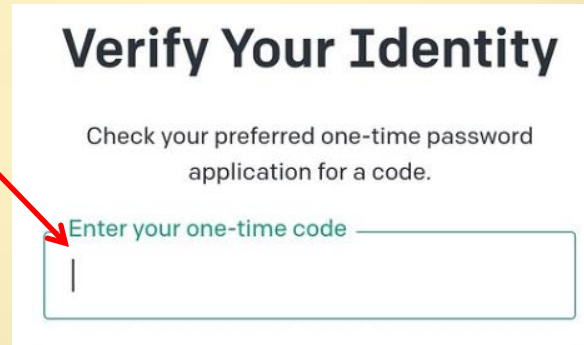
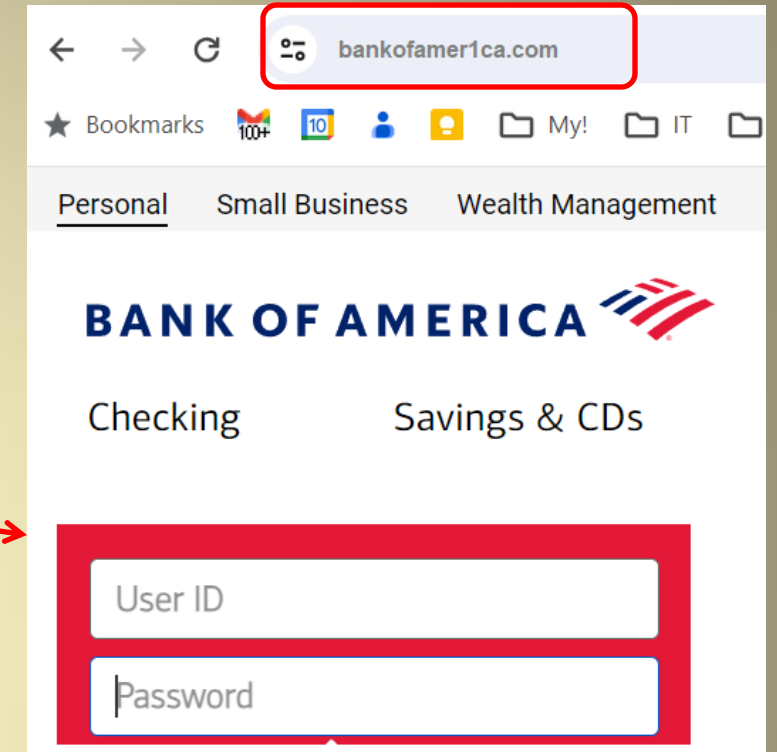
**Step 2:** You enter your username and password.  
Scammer enters your credentials on the REAL BofA site

**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

Is your phone unlocked when within range of your watch?

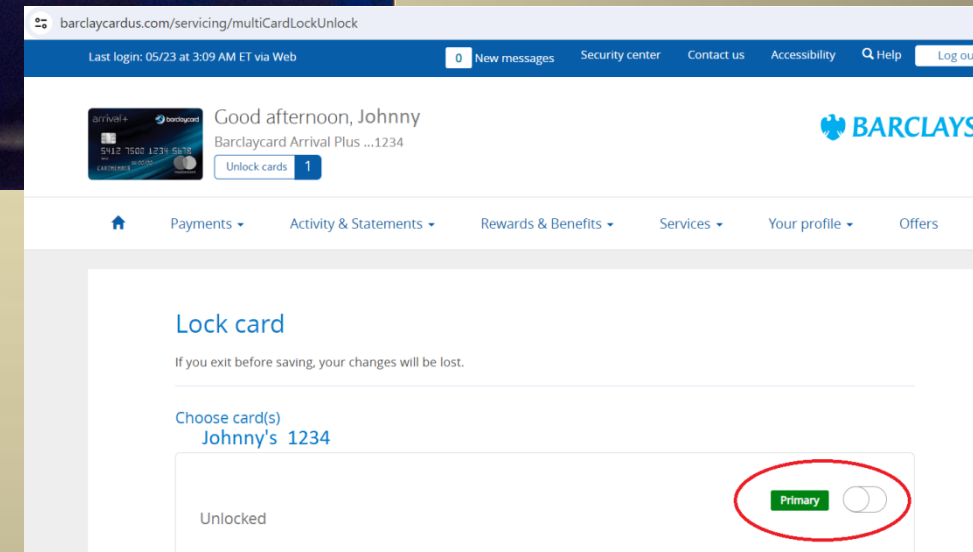
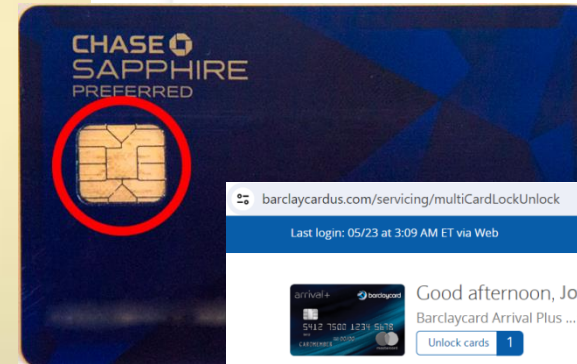
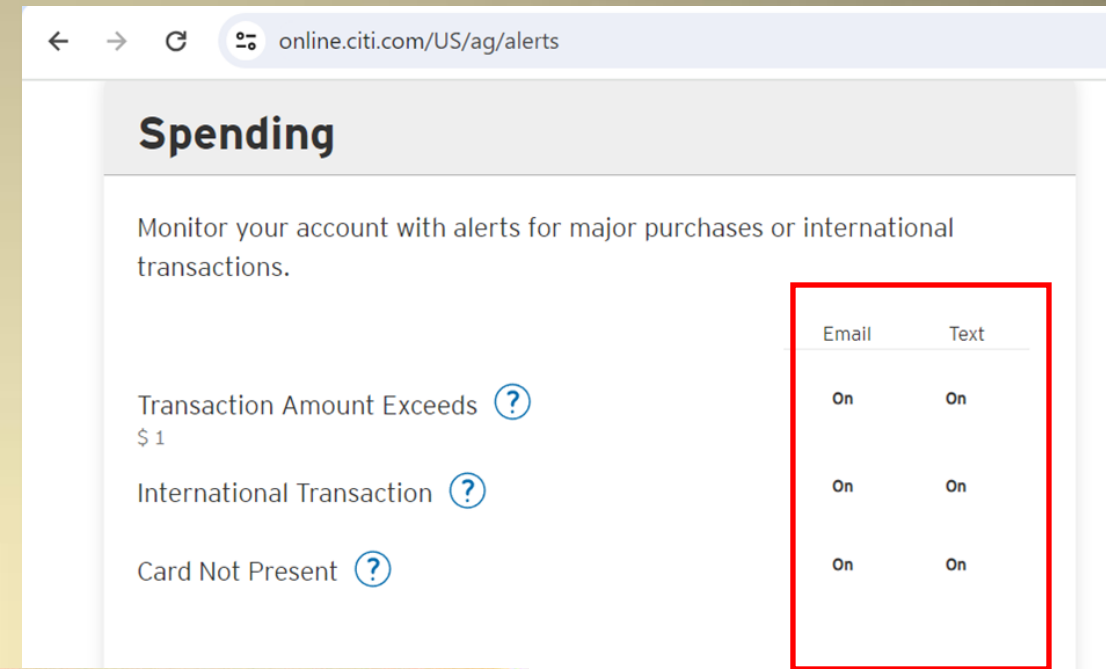
- Phone can stay unlocked within range of your watch
- **Recommend: Use a fingerprint, PIN or pattern (rather than facial recognition) to unlock your phone**

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

- **Setup text/email alerts** for your credit cards
- Same with your bank, investment accounts
- Bank ATMs are more secure than retail ATMs
- Be careful of devices with skimmers
  - Inspect device before using your card
- Cards with EMV chips are harder to clone
  - Use a **chip reader or tap** rather than 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

## What Should You Do if Your Information is Compromised?

Call each of the credit bureaus and put a hold on your credit that requires your authorization to unfreeze

- TransUnion
- Equifax
- Experian

TransUnion<sup>tu</sup>

**EQUIFAX**

experian<sup>TM</sup>



Credit **Freezes** are free! [**Locks** are not free but freezes are effective]

- Limits access to your credit to those you currently have accounts with
- **Prevents anyone from opening an account in your name**
- Unfreeze temporarily to open a new account

# 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

## Security Freeze

Placing, temporarily lifting, or removing a security freeze is free.

PLACE A SECURITY FREEZE

MANAGE A FREEZE

### Let's get started

We'll need some of your information first.

Already have an account? [Sign in here](#)

#### Personal information

First name

Last name

Date of birth (MM/DD/YYYY)

SSN or ITIN (XXX-XX-XXXX)

Your Social Security number helps us locate your credit report and verify your identity.

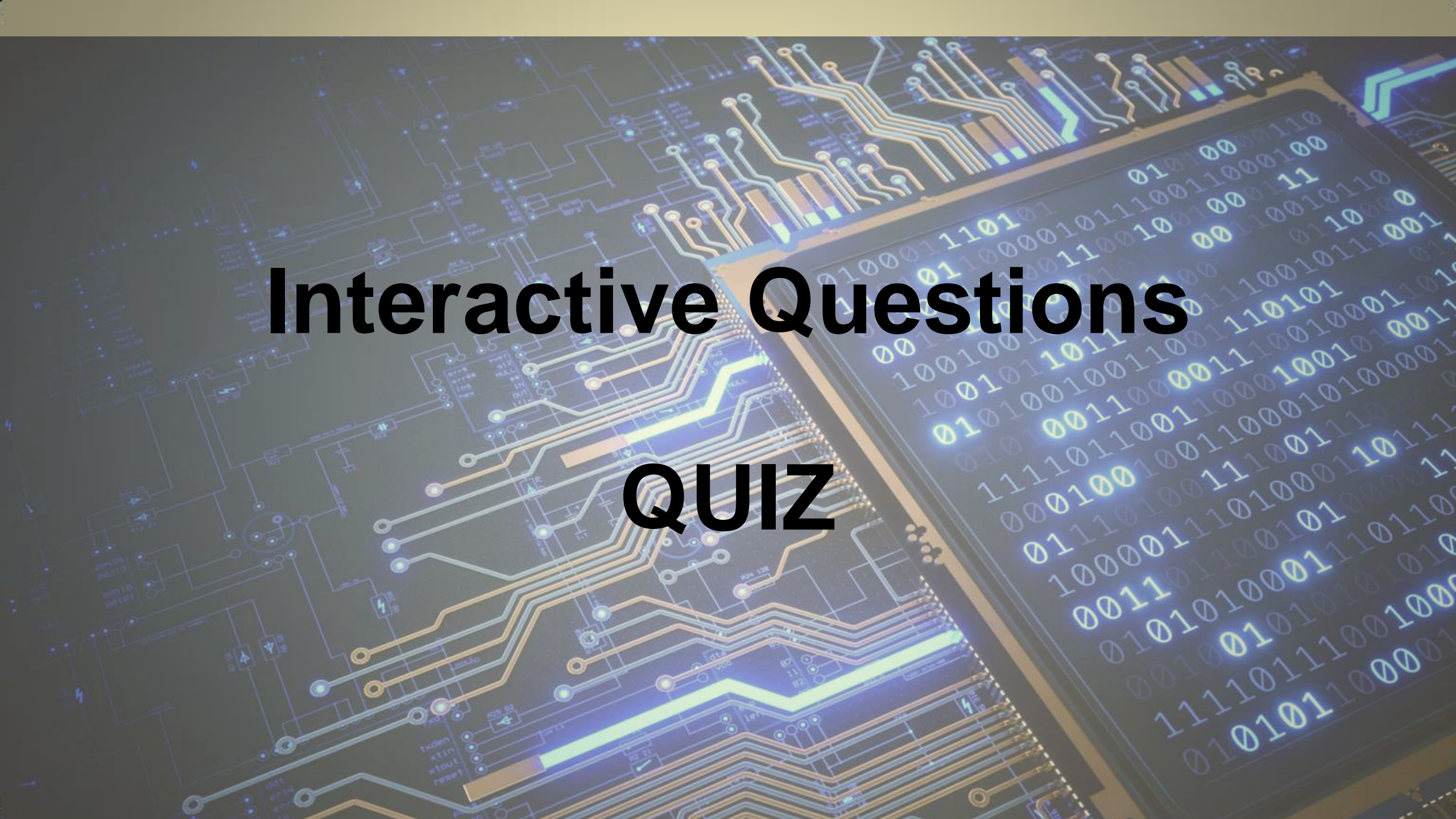
Mobile number (XXX-XXX-XXXX)

We may text you to verify your identity and to provide service-related alerts. Message and data rates may apply. If you do not have a mobile number, use your home phone number.

You have **temporarily lifted** your Equifax credit report freeze through **06/16/2024**.

MANAGE A FREEZE





# Interactive Questions

## QUIZ

## **Question: Safe Links**

**Scenario:** You receive an email from your bank. Which link is safer to click?

- **Option A:** "Click here to verify your account details:  
[www.bank-secure-login.com](http://www.bank-secure-login.com)"
- **Option B:** "Visit our website and log in to your account:  
<http://www.bankofamerica.com>"

**Answer: Neither.**

The link text can be misleading and obscure a fraudulent link. Use a bookmark you've previously saved, or type in the official bank URL into the browser.



## **Question: Strong Password**

**Scenario:** Which of the following is a stronger password?

- **Option A:** "Password123"
- **Option B:** "T3x!7K\$z#9Qw"
- **Option C:** "workHard79"

**Answer: B**

B is longer and includes upper/lower case letters, numbers and special characters.

## Question: Phishing Email

**Scenario:** You receive an email claiming you've won a prize. What should you do?

- **Option A:** Click the link in the email to claim your prize.
- **Option B:** Verify the sender's email address and contact the company directly through their official website.
- **Option C:** Check if the company is legitimate before you go to their website or enter personal information.

**Answer:** Most such emails are scams.

But if you really must follow through, Option C is best.

Do not click any links or download attachments.

## Question: Public Wi-Fi Safety

**Scenario:** You're at a coffee shop and need to check your bank account. What's the safest way to do this?

- **Option A:** Use the coffee shop's free Wi-Fi to log in to your bank account.
- **Option B:** Use your mobile data or a VPN (Virtual Private Network) to access your bank account.

### **Answer: B**

Public Wi-Fi networks are often insecure and can expose your personal information to hackers. Using mobile data or a VPN ensures a more secure connection to your bank account.



## Question: Software Updates

**Scenario:** You receive a notification that there is a software update available for your device. What should you do?

- **Option A:** Continue using your device.
- **Option B:** Install the update as soon as possible to ensure your device is secure.

### **Answer: B**

Software updates often include important security patches that protect your device from vulnerabilities and enhance overall performance.

## **Question: Social Media Privacy**

**Scenario:** You want to share a vacation photo on social media. What is the best practice?

- **Option A:** Share the photo publicly.
- **Option B:** Share the photo with a select group of friends using privacy settings.

### **Answer: B**

Consider posting photos after your trip to avoid revealing your current location and travel schedule.

You can enjoy sharing your vacation memories while maintaining your privacy and security.

## **Question: Two-Factor Authentication (2FA)**

**Scenario:** Which of the following provides better security for your online accounts?

- **Option A:** Password only.
- **Option B:** Password and a verification code sent to your phone.
- **Option C:** Password and a code from an authenticator app.
- **Option D:** Password, a code and a hardware key.

### **Answer: D**

This option combines multiple layers of security, including something you know (the password), something you have (the code), and something you possess (the hardware key).



## **Question: Suspicious Attachments**

**Scenario:** You receive an email with an attachment from an unknown sender. What should you do?

- **Option A:** Open the attachment to see what it is.
- **Option B:** Delete the email or mark it as spam without opening the attachment.

## **Answer: B**

Attachments from unknown senders can contain malware or viruses. It's safest to delete the email or mark it as spam to protect your device and personal information.

## Question: Password Management

**Scenario:** How should you manage your passwords for different accounts?

- **Option A:** Use one password for all accounts to make it easier to remember.
- **Option B:** Use a password manager to generate and store unique passwords for each account.
- **Option C:** Use a variation of a “root” password slightly modified for different accounts.

### **Answer: B**

Using a password manager ensures that each of your accounts has a strong, unique password, reducing the risk of security breaches. It also simplifies the process of managing multiple passwords, as you only need to remember one master password for the password manager.

## **Question: Safe Browsing**

**Scenario:** You come across a website offering a free download of a popular software program. What should you check before downloading?

- **Option A:** Download the software to take advantage of the offer.
- **Option B:** Verify the legitimacy of the website and check for reviews or official sources before downloading.

### **Answer: B**

Look for official or well-known sources like the software's official website or reputable download sites. (Game software is particularly risky.)





# Recommendations and Additional Resources

# 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

## SCAM ALERT

Scammers and cyber criminals are using the COVID-19 outbreak to take advantage of victims.





# 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

IF YOU ARE A VICTIM

# 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](https://reportfraud.ftc.gov)
  - Call the AARP Fraud Watch Network Helpline [877-908-3360](tel: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=AmUC4m6wIwo>



**THANK YOU**

QUESTIONS?