Carefull



How to Stay Safe Online

Cameron Huddleston, Carefull

April 22, 2025

Americans lose more than $12.5 billion annually to cybercrime.

Source: FBI Internet Crime Complaint Center

How Thieves Steal Your Money and Information Online

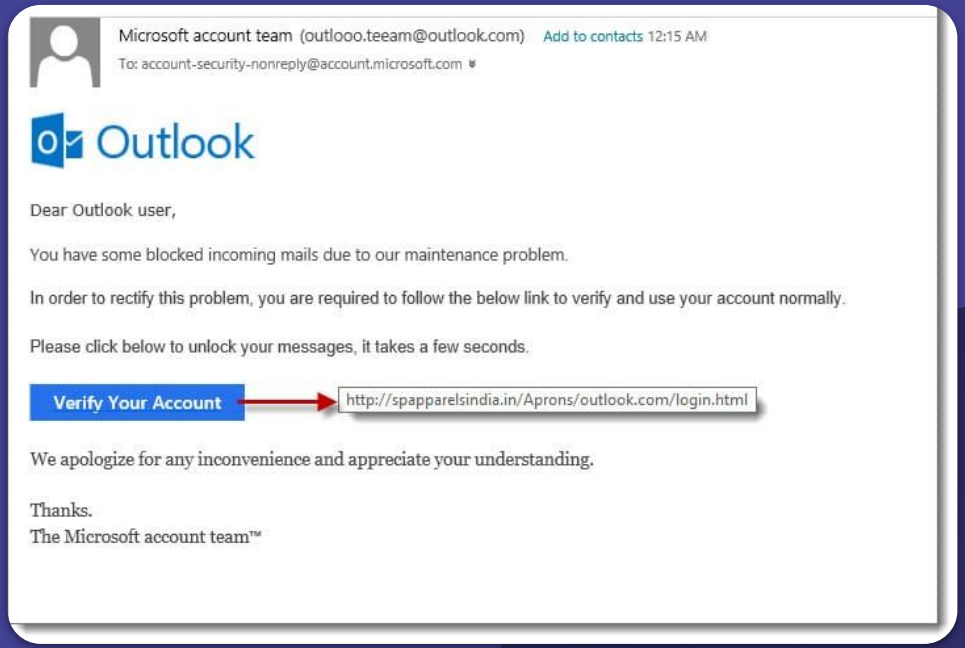


Phishing Emails

Email is the most common way scammers make contact with potential victims.*

Phishing emails typically appear to come from businesses, government agencies and well-known organizations.

Messages include an urgent call to action with a prompt to click a link to a site that will steal your personal information or money or to download a file that includes spyware.



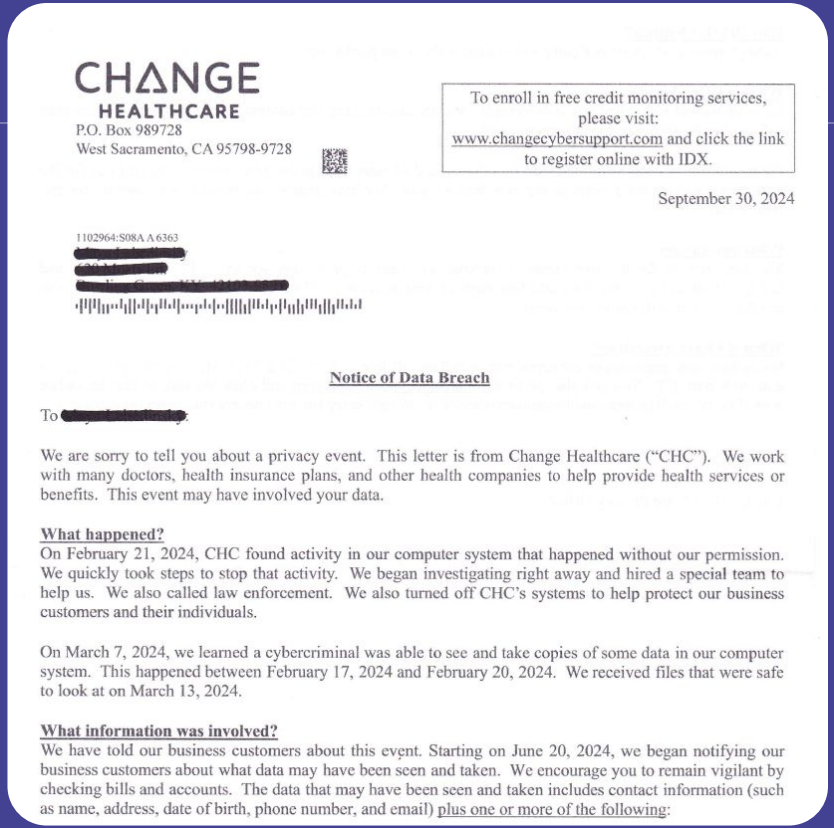
Source: Federal Trade Commission

Data Breaches

Hackers gain access to company databases that include personal and account information of customers.

There were 3,158 data breaches reported in 2024.* It can take companies months to alert consumers about breaches.

Hackers can use the information to steal identities and access accounts, or they sell the information on the dark web.



CHANGE HEALTHCARE
P.O. Box 989728
West Sacramento, CA 95798-9728

To enroll in free credit monitoring services, please visit: www.changecybersupport.com and click the link to register online with IDX.

September 30, 2024

1102964:S08A A 6363
[redacted]

Notice of Data Breach

To [redacted]

We are sorry to tell you about a privacy event. This letter is from Change Healthcare ("CHC"). We work with many doctors, health insurance plans, and other health companies to help provide health services or benefits. This event may have involved your data.

What happened?
On February 21, 2024, CHC found activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began investigating right away and hired a special team to help us. We also called law enforcement. We also turned off CHC's systems to help protect our business customers and their individuals.

On March 7, 2024, we learned a cybercriminal was able to see and take copies of some data in our computer system. This happened between February 17, 2024 and February 20, 2024. We received files that were safe to look at on March 13, 2024.

What information was involved?
We have told our business customers about this event. Starting on June 20, 2024, we began notifying our business customers about what data may have been seen and taken. We encourage you to remain vigilant by checking bills and accounts. The data that may have been seen and taken includes contact information (such as name, address, date of birth, phone number, and email) plus one or more of the following:

Source: Identity Theft Resource Center

Tech Support Scams

A pop-up message appears on your computer claiming there is a virus or suspicious activity and a number is provided for tech support.

If you call the number, a “technician” will ask for remote access to your computer to fix the problem.

With remote access, the scammer can get into your email and any accounts with saved passwords.



Online Shopping Scams

Scammers post ads online for deeply discounted goods with links to fake retail sites or replicas of actual retailers' sites.

Scammers pose as buyers and sellers on online marketplaces such as Facebook Marketplace.

Scammers use AI to create images or videos of celebrities promoting products that are fake.

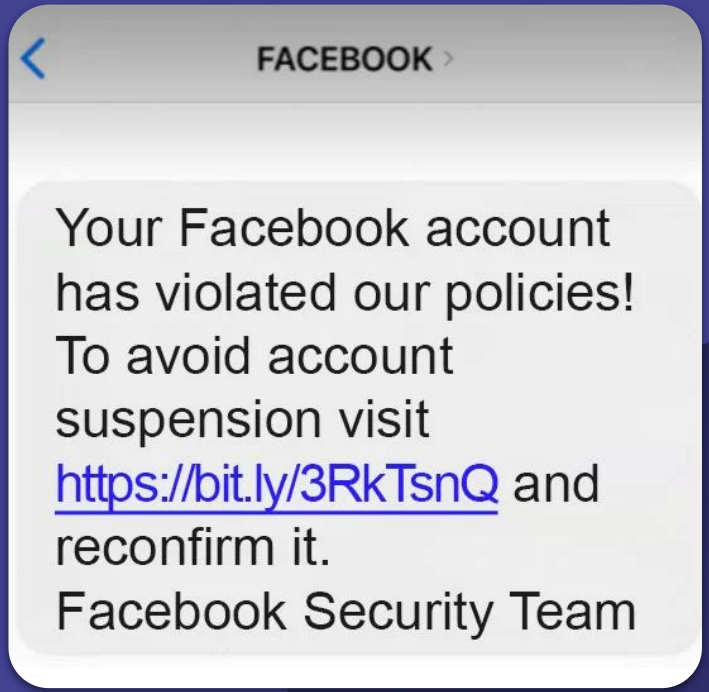


Social Media Scams

Scammers post fake giveaways, solicit charitable donations, offer invites to investment clubs, and share links to fake live streams for funerals and other events.

Scammers create fake profiles using stolen photos to strike up romances and ask for money.

Scammers send messages that appear to come from Facebook with warnings that your account is compromised and a link to provide or reset your login credentials.



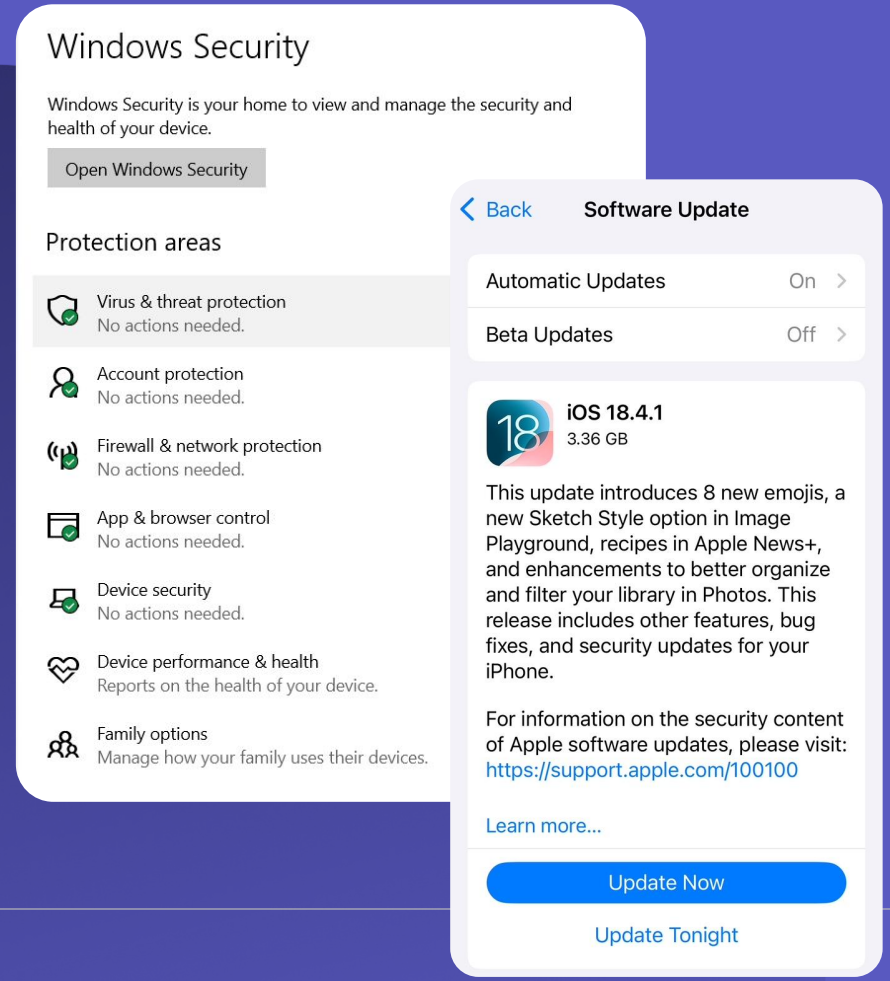
How to Stay Safe

- Minimize Risk of Exposure
- Monitor for Fraud
- Minimize Damage



Minimize Risk

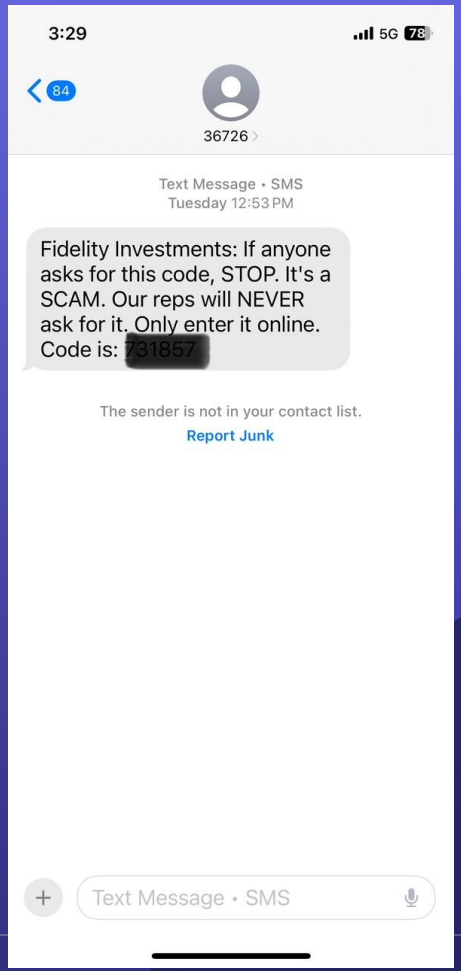
- Keep antivirus software updated on your computer.
- Run operating system updates on your phone.
- Keep privacy and security settings on your Internet browser updated.
- NEVER grant remote access to your computer.





Minimize Risk

- Set up online access to accounts.
- Use strong passwords that are at least 12 characters long with upper- and lowercase letters, numbers and symbols.
- Use a different password for every account. A password manager can create and securely store passwords.

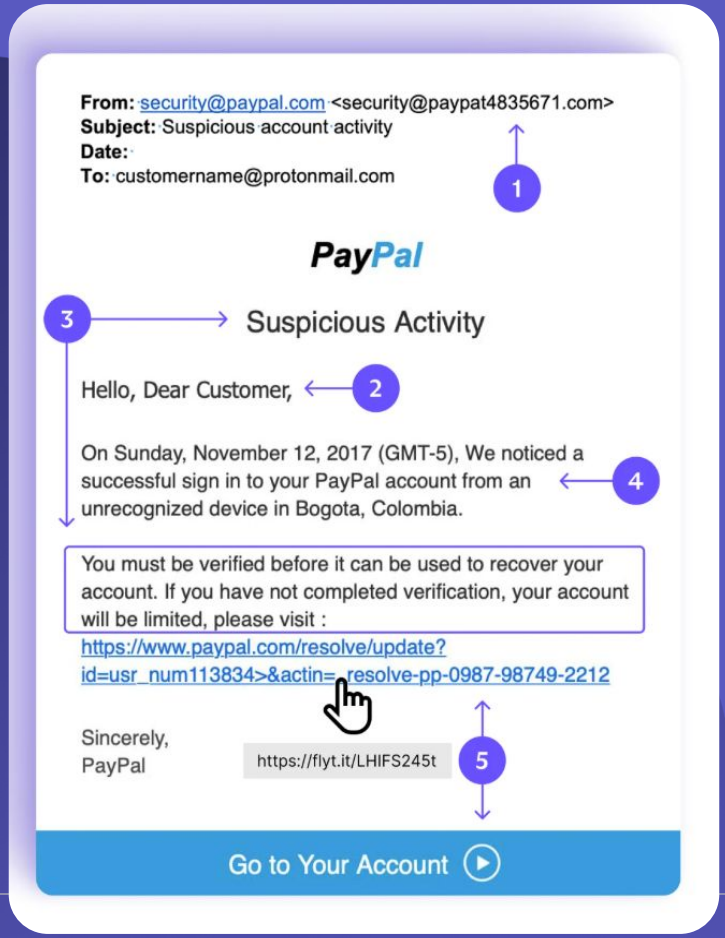


Minimize Risk

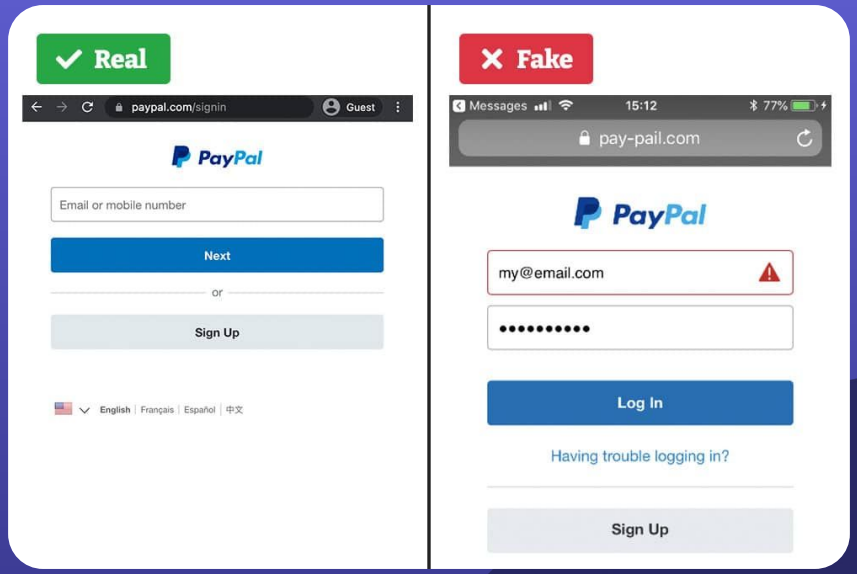
- Use multi-factor authentication (MFA).
- MFA is a security feature that requires you to provide identity verification in addition to a password—such as a code sent by text message.
- Your financial institutions and online account providers should offer the option to opt into MFA.
- Your financial institution will never call and ask for your MFA code. This is a tactic scammers use.

Minimize Risk

1. Check the email address to make sure it matches the company name.
2. Look for generic greetings.
3. Be wary of urgent requests.
4. Look for spelling, grammar and punctuation mistakes.
5. Don’t click on links or attachments.



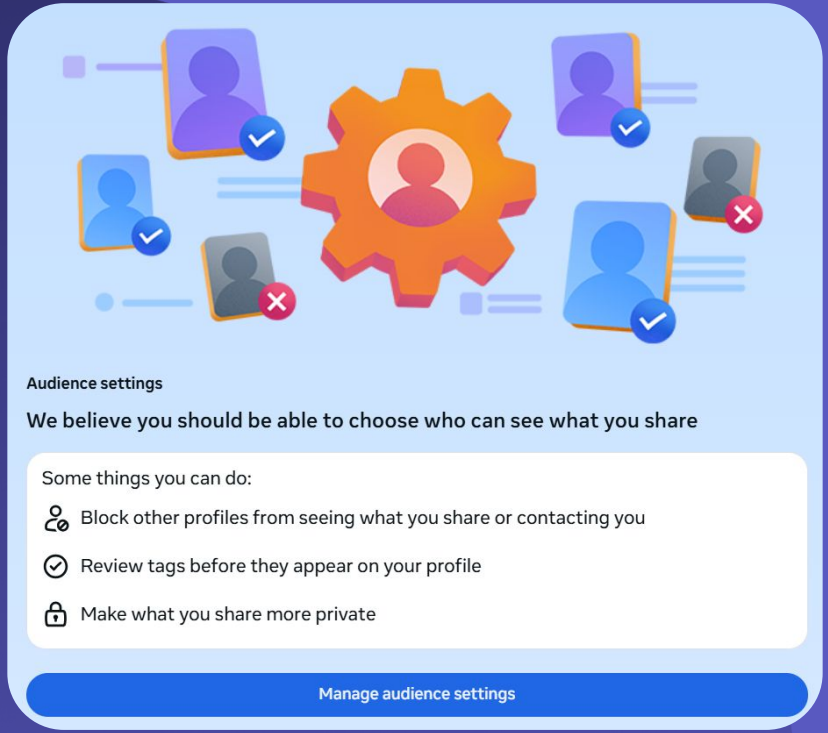
Minimize Risk



- Stick with online retailers you know and trust.
- Don’t click on ads or sponsored results.
- Read reviews and search for complaints before shopping on unfamiliar sites.
- Look for https:// and the padlock symbol and check the domain name. Beware of URLs ending in .shop, .vip, .link.

Minimize Risk

- Adjust privacy settings on social media sites to limit who can see your posts.
- Be careful what information you share because scammers can use it.
- Don’t click on ads or posts for products on social media.
- Be wary of strangers who contact you with friend requests, special offers or donation requests.



Monitor for Fraud



Check financial accounts regularly — don’t wait for monthly statements.

Check your credit reports for free at Annualcreditreport.com to look for loans and lines of credit you don’t recognize.

Use credit and identity monitoring to be alerted to changes in your credit reports and misuse of your information.

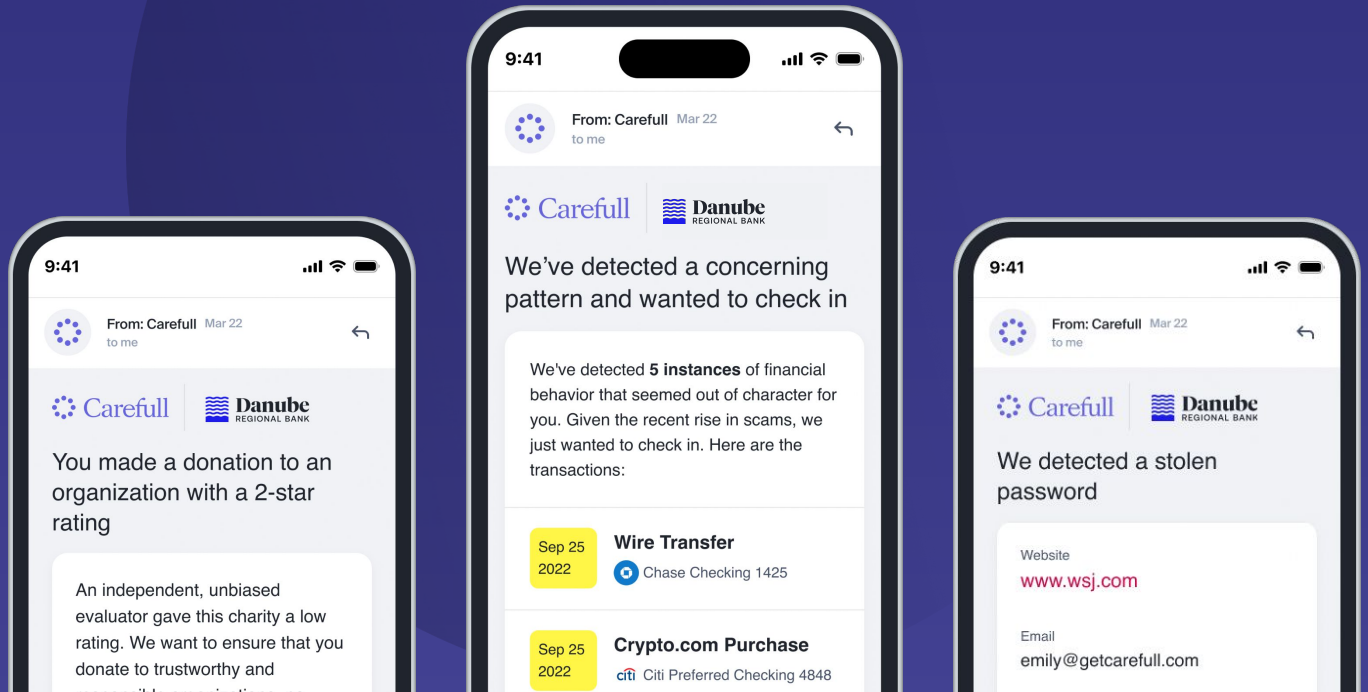
Monitor your mail for unusual bills or collection notices.

Check health insurance statements for services you didn’t receive or denial of coverage for reaching benefit limits.

Stay alert to notices about unfamiliar account login attempts. Contact your account provider directly.

How Carefull Can Help

Account Monitoring	Credit Monitoring	Identity Monitoring	Home Title Monitoring	Scam Check	Data Breach Detection



Minimize the Damage







Report

Report fraudulent transactions to financial institutions immediately.

Report identity theft to local law enforcement and IdentityTheft.gov.

Report identity theft to IRS, Medicare, Social Security Administration if necessary.

Secure

Cancel credit or debit cards that have been compromised.

Change passwords for compromised accounts.

Place a security freeze on your credit reports at Equifax, Experian and TransUnion.

Repair

Contact companies to close new accounts opened in your name.

Ask companies to remove fraudulent transactions from your account.

Contact the credit bureaus to have fraudulent accounts removed from your reports.

Always ...

- Question unsolicited communications
- Verify the identity of anyone who asks for money or personal information
- Never rush into making payments

Carefull

care@getcarefull.com