Keeping your personal information safe online

MERRILL
A BANK OF AMERICA COMPANY

Cyber criminals have become more sophisticated in their attempts to steal your identity. Identity (ID) theft occurs when someone gains access to personal information, such as name, date of birth, address and Social Security number, and uses that information to commit fraudulent crimes. That's why it's important for you to know what to do if you become an ID theft victim.

I think I might be a victim of identity theft. What steps should I take?

Here are some important steps you can take right away if you believe your identity has been compromised:

- **Contact your financial institutions and creditors.**
  Speak with their fraud departments and explain that someone has stolen your identity.
- **Check your credit reports and place a fraud alert on your file.**
  Initiate a fraud alert by contacting one of the three credit bureaus (when you contact one credit bureau, the other two bureaus are notified automatically). Review these reports closely for inaccuracies and close any accounts you believe were opened fraudulently.
- **File an identity theft report and retain it for your records.**
  Complete a report online at the Federal Trade Commissions (FTC) identity theft website and contact your local law enforcement to report the crime.
- **Protect your device against malware or malicious software.**
  Download and install security software that updates automatically from a reputable company you trust.
- **Change your passwords and PINS.**
  Make sure to change your online sign-in credentials, passwords and PINs on all of your accounts at financial institutions, including Bank of America and Merrill Lynch.
- **Set up account and security alerts.**
  Receive notifications of activity on your accounts so you can take action immediately and protect yourself against fraud.
- **Replace your stolen identification.**
  If your driver's license has been stolen, please contact your local Department of Motor Vehicles to report and replace it. Check to see if a secondary license has been issued in your name.

Visit Merrill's Security Center for additional tips and tools on how to increase your security, and stay protected against fraud and scams.

Check your credit reports annually

Equifax®
1.888.766.0008 www.Equifax.com

Experian®
1.888.397.3742 www.Experian.com

TransUnion®
1.800.680.7289 www.transunion.com

If your identity has been compromised

Contact the Federal Trade Commission (FTC). The FTC will enter your complaint information into its Consumer Sentinel Network database and provide victim assistance and consumer education materials. Its website has information about your rights as a victim of identity theft and explains the steps needed to repair your name and credit.

The Federal Trade Commission (FTC)
1.877.IDTHEFT (438.4338) www.ftc.gov/idtheft

If your Social Security number has been compromised

Consider contacting the Social Security Administration and the IRS as well as one of the three credit bureaus listed below, and consider putting a fraud alert or credit freeze on your file at the bureaus to limit access to your credit report.

Social Security Administration Fraud Hotline
1.800.269.0271

Internal Revenue Service (IRS)
1.800.908.4490 www.irs.gov

My Merrill account may have been compromised. What should I do?

Here are some online security tips and best practices to follow if you think your Merrill account has been compromised:

- If you notice suspicious or fraudulent activity on your account, notify your Merrill Financial Advisor 1.800.MERRILL (1.800.637.7455) and have a Relationship Pin (RPIN) placed on your account immediately.
- Review all recent activity in your account(s) to make sure no further fraudulent activity has occurred.
- Add a security code/PIN to your smartphone. If your device offers the capability to enable fingerprint or other biometric authentication, this should be enabled as well.
- Set up an alternative delivery option to receive a one-time code used when logging into the Merrill website and mobile application.

How can I be sure my email to my financial advisor and client associate are safe?

Use MyMerrill Secure Message Center for communications with your financial advisor or client associate. Unlike regular email, the Secure Message Center is protected by Merrill firewalls and requires you to login to MyMerrill using your User ID and password to send an email to your financial advisor and client associate through the Secure Message Center.

My email has been compromised. What should I do first?

Your e-mail account has been compromised if an unauthorized person acquired your login information, and has used it to access your e-mail account potentially to commit fraud. If you think your email account has been compromised, in addition to changing your login credentials, take these steps as soon as possible:

- **Determine if any fraudulent emails were sent from the compromised account.**
  Check the account's "sent" and "deleted" folders to check for any emails you didn't write. Often, you learn you were compromised when someone on your contact list alerts you that he or she received an email from your account containing a suspicious link or other questionable information.
- **Notify your contacts**.
  Let them know they may receive spam messages that appear to come from your email account, and to not open those messages or click on any links they might contain.
- **Determine if any sensitive information might have been compromised.**
  Sensitive information includes Social Security numbers, passwords, account numbers and/or other financial Information.

What should I do if I receive a suspicious email?

If you do receive a suspicious email, don't click on any links in it or reply to it—simply delete it.

To report a suspicious email that uses Merrill or Bank of America's name, forward it to abuse@bankofamerica.com.

And, to make sure you're at MyMerrill.com website when you log in to your account, type www.mymerrill.com in your browser.

Tips for creating strong login credentials

Avoid using common information.
Instead of using the word "password," your name, birthday, Social Security number, or your pet's name, use something that's meaningful to you but isn't common knowledge.

Use at least 8 characters and include letters, numbers, punctuation and symbols.
The greater the variety of characters in your password, the better. For example, "P@SSw0rD" is more secure than "password" but "2P!nkC@tS" is even better.

Use different passwords for different sites and change your passwords often.
Cyber criminals often steal passwords on websites that have very little security and then use that same password and username in more secure environments, such as banking websites. Set up an automatic reminder to change your passwords every three months for your email, banking, credit card and social media accounts.

Use your security questions regularly, choosing questions and answers that are unique to you.
The information you provide identifies you and helps protect you from fraud.

Multifactor Authentication

Sometimes called "multifactor authentication," this process uses two steps to check the identity of an individual trying to access an email account, computer or network, such as a username/password and a four-digit numeric code texted to the account holder.

Increase your overall security and add an extra layer of protection with multifactor authentication.

How do I avoid getting malware on my computer?

Malware is often used to steal personal information and to commit fraud. Here are some ways to help avoid getting malware on your computer:

- Don't download files from file sharing and social networking sites — these sites can be distribution points for malware.
- Don't open or install any file/document attachment or free software from unknown sources.
- Don't click on pop-ups that ask for personal or financial information.

What can I do to make my computer more secure?

- **Install and use malware protection software.**
  Merrill offers free IBM® Security Trusteer Rapport™ malware protection software. For more information about Trusteer Rapport™, visit the site listed in the box on the right.
- **Install and use anti-virus and anti-spyware protection.**
  This software detects and removes viruses and spyware, which can steal vital information. Run full system scans regularly instead of relying on quick scans.
- **Make sure your computer's firewall is on.**
  A firewall puts a protective barrier between your computer and the Internet, and turning it off for even a short time increases the risk that your computer could be compromised. More information on activating this feature should be obtained from your computer's manufacturer.
- **Install operating system and software updates as soon as possible.**
  Allow your computer to install updates automatically or at regularly scheduled intervals to keep your system current.

How can I make my browsing experience safer?

Is your web browser up-to-date? If not, updating your computer, phone or tablet with the most recent version can help you stay protected while you're online.

For your online safety, avoid using free and public Wi-Fi connection for banking transactions. It is more secure to use legitimate banking apps over a cellular network. And, if available, use a virtual private network (VPN) to protect your data so your login credential aren't compromised by someone else using the same public Wi-Fi network. VPN provides security so that traffic sent through the VPN connection stays isolated from other computers on the network. *Due to AML regulations — some VPN transactions may be restricted.*

Visit Merrill's Security Center for additional tips and tools on how to increase your security, and stay protected against fraud and scams.

Malware

Short for "malicious software," it includes viruses, spyware, worms and trojans that are designed to infiltrate or damage a computer system.

Protect yourself with IBM® Security Trusteer Rapport™

Trusteer Rapport™ online fraud protection software is free from Merrill Lynch and helps protect you from malware and phishing attacks. Installing Trusteer Rapport™ is fast and easy.

Download now

Know the difference between Spoofing and Phishing

Spoofing
Impersonating a reputable person or company you may have a relationship with (such as Bank of America or Merrill) — often with the goal of getting you to click on a link or open a file that downloads malware onto your system.

Phishing
An attempt to get you to reveal personal, sensitive information (such as your Social Security number or account passwords) to the cyber criminal, who will use that information for financial gain.

Is that banking mobile app legitimate? Three tell-tale signs:

1. The mobile app's author or developer is the bank itself.
2. The mobile app is offered on the official app store for your mobile device.
3. The mobile app is free. If you're being asked to pay for the download, confirm with your bank first — most mobile banking apps are free.

Stay Safe Online website offers additional information at www.staysafeonline.com.

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

Android is a trademark of Google, Inc.
Equifax is a registered trademark of Equifax, Inc.
Experian is a registered trademark of Experian Information Solutions, Inc.
IBM and *Trusteer Rapport* are trademarks of the International Business Machines Corporation.
iPhone is a registered trademark of Apple, Inc.
TransUnion is a registered trademark of TransUnion LLC.

Merrill may include links to third party sites as a convenience. Merrill has not endorsed or approved the content on any sites that are not owned or managed by Merrill, and does not monitor or maintain any of the site's information. When you visit the site from this link, you are agreeing to all of its terms of use, including its privacy policies.