Keeping your personal information safe online

While living in a digital age has its advantages, it also comes with risks. As cybercriminals have become more sophisticated in their attempts to get our personal data, it's become increasingly important to protect our digital devices and use the Internet safely and securely.

Whether you want to protect your Merrill Lynch account (page 1), increase your computer's security (page 2), are trying to identify signs of spoofing and phishing (page 3), think your identity might have been stolen (page 4), or if you've been hacked and aren't sure of your next steps (pages 5–6), we have some tips that can help.

My Merrill Lynch retirement account/brokerage account has been compromised. What should I do?

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

- If you notice suspicious or fraudulent activity on your retirement or brokerage account, notify Merrill Lynch immediately.
- Run a virus scan on all of the computers you have used to access the account(s) in order to check for viruses/malware (key logging software). Do this before changing your login credentials.
- Review all recent activity in your account(s) to make sure no further fraudulent activity has occurred.
- Call the Retirement and Benefits Contact Center at 1.800.228.4015 and have a verbal password placed on your account.
- Add a security code/PIN to your smartphone. For iPhone® users, you can find a Passcode option under "Settings." For Android™ phones, go to "Settings" and select "Security."
- Add fingerprint verification to your device if it offers this option. Most Apple® and Android™ devices have a fingerprint scanner with this capability. For Apple® devices, the option to establish this service can be found under "Settings"; for Android™ devices you must select "Settings" and then "Security."

Consider contacting the agencies at right if your Social Security number was compromised.

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

Equifax®
1.888.766.0008
www.equifax.com

Experian®
1.888.397.3742
www.experian.com

TransUnion®
1.800.680.7289
www.transunion.com

How do I avoid getting malware on my computer?

Malware is often used to steal personal information and to commit fraud. Here are three 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 attachments or free software from unknown sources.
- Don't click on pop-up advertisements that ask for personal or financial information.

What can I do to make my computer more secure?

- Install and use malware protection software.
  Merrill Lynch offers free IBM® Security Trusteer Rapport™ malware protection software. For more information about Trusteer Rapport™, visit the site listed in the box to 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.
- Install operating system and software updates as soon as possible.
  Consider allowing 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 — such as Internet Explorer®, FireFox®, Safari® and Chrome™ — up-to-date? If not, installing the most recent version, and regularly updating your computer, phone or tablet can help protect you when you're online.

If you're using free public Wi-Fi, try to use Secure Socket Layer (SSL) login pages whenever possible. SSL is a security protocol that enables websites to pass along sensitive information securely in an encrypted format. SSL-protected pages have "https://" instead of "http://" at the beginning of their URL, and they typically include an image of a lock or other icon to show that your connection to the site is secure.

And, if available, use a virtual private network (VPN) to protect your data so your login credentials 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 intermediate network.

The National Cyber Security Alliance website offers additional information at www.staysafeonline.org.

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. Visit http://www.ibm.com/security/trusteer/landing-page/benefitsonline/ and click on the "Download now" button.

What's the difference between phishing and spoofing?

You may have heard the terms "phishing" and "spoofing" used together, but they're actually two different ways cybercriminals try to trick you.

For example, cybercriminals may send you an e-mail that looks like it has come from Merrill Lynch or Bank of America (spoofing). These phony e-mails ask you to go to a fake website that looks like Merrill Lynch or Bank of America (spoofing) and to provide your personal retirement or brokerage account information (phishing). These e-mails may even ask you to call a phone number and provide your retirement or brokerage account information (phishing).

Merrill Lynch or Bank of America will never ask you to reply in an e-mail with any personal information, such as your Social Security number or the PIN for your ATM or debit card.

What are some signs that I'm being "phished" or "spoofed"?

- The e-mail or website may contain typos, grammatical error, awkward writing and poor visual design. Check both the content of the e-mail and the subject line that appears in your inbox, as well as the URL of the site.
- The sender's e-mail address isn't affiliated with the bank, brokerage firm or company they're pretending to represent. Cyber criminals sometimes use e-mail addresses that are similar to legitimate companies, adding extra numbers or characters to a company's e-mail address or domain name.
- You receive an urgent appeal that claims your retirement or brokerage account may be closed or that you will be fined if you fail to confirm, verify or authenticate your personal information.
- You get a message directing you to update your retirement or brokerage information online due to system and/or security upgrade.
- Offers that sound too good to be true often are. You may be asked to fill out a short customer service survey in exchange for money being credited to your bank account, and are then asked to provide your bank account number for proper routing of the supposed credit.

What should I do if I receive a suspicious e-mail?

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

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

And, to make sure you're at Merrill Lynch's Benefits Online® website when you log in to your retirement account, type www.benefits.ml.com in your browser.

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

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

Spoofing

Impersonating a reputable person or company you may have a relationship with (such as Bank of America or Merrill Lynch) — often with the goal of getting you to click on a link 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 cybercriminal, who will use that information for financial gain.

Look for a green "lock" icon, "https://" and a green bar in your web address each time you log into a secure site, such as your Merrill Lynch account or an online store.

These three items are proof of the website's security certificate, which verifies that you are connected to a secure site operated by its true owners and that any data sent between you and website is encrypted. If you don't see these items, double-check that you have typed the correct address in your web browser.

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

Identity theft is a serious crime that can have far reaching effects, from a negative impact on your credit rating to financial loss and personal ruin. If you think your identity has been stolen, take these steps immediately:

- Contact the agencies listed in the box on page 1.
- Place a fraud alert and/or credit freeze on your account at one of the three credit agencies.
  Doing so entitles you to a free credit report from each bureau. Review these reports closely for any inaccuracies, and close any accounts you believe were opened fraudulently.
- Change your PINs and passwords on all of your accounts at financial institutions, such as your bank account or Merrill Lynch retirement and/or brokerage account.
- File a police report and get a copy.
  The police report should include all of the fraudulent activity as well as the identity theft. The credit bureaus will accept a copy of the police report to block any fraudulent account information from appearing on your credit report.
- Contest all fraudulent accounts in writing.
  Follow up with the financial institution/business by sending the FTC's Identity Theft Affidavit found on the FTC website. See the box to the right for the FTC's website.
- Contact the Department of Motor Vehicles.
  Check to see if a secondary driver's license has been issued in your name.
- Contact your phone provider(s).
  Place a PIN number on your phone account(s) to prevent call forwarding.
- Run an up-to-date full system virus scan on your computers.
  You'll want to check each computer that you used to access your banking, retirement and brokerage accounts for viruses and malware, including key logging malware.

Consider downloading Trusteer Rapport™ online fraud protection software. See the box on page 2.

Identity theft

When criminals obtain sensitive information about you, such as your name, Social Security number or financial data, and then use that information to commit fraud or other crimes.

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 (1.877.438.4338)

www.ftc.gov/idtheft

My e-mail has been hacked. What should I do first?

Your e-mail account has been compromised — or "hacked" — 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 e-mail account has been hacked, take these four steps as soon as possible:

1 Determine if any fraudulent e-mails were sent from the compromised account.
Check the account's "sent" and "deleted" folders to check for any e-mails you didn't write. Often, you learn you were hacked when someone on your contact list alerts you that he or she received an e-mail from your account containing a suspicious link or other questionable information.

2 Notify your contacts.
Let them know they may receive spam messages that appear to come from your e-mail account, and to not open those messages or click on any links they might contain.

3 Determine if any sensitive information might have been compromised.
Sensitive information includes Social Security numbers, passwords, account numbers and/or other financial Information.

4 Run an up-to-date, full-system virus scan on all of your computers.
Run the scan before you change your e-mail login information — if there's a virus or malware on your computer, it might be able to continue to access your e-mail account even if you change your login. Consider contacting a computer professional for assistance; sophisticated malware can conceal itself from anti-virus programs and, in some cases, prevent them from working altogether.

Should I keep the compromised e-mail account or close it?

If you've been hacked, the most secure option is to close down the compromised e-mail account and open a new one. Consider creating a "throw-away" e-mail account for websites where you only want to access the site once or twice, and an e-mail account that you only use for secure sites, such as banking and credit cards.

For more information about securing your computer and preventing malware, see page 3.

Tips for creating a strong password

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 8–10 characters and include letters, numbers, punctuation and symbols.
The greater the variety of characters in your password, the better. For example, "P@$$w0rD" is more secure than "password" but "2P!nkC@t$" is even better.

Use different passwords for different sites and change your passwords often.
Cybercriminals 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 e-mail, banking, credit card and social media accounts.

I want to keep my e-mail account that was compromised; I have a lot of information in it. What should I do?

If you decide to keep the hacked e-mail active, taking these steps can help you regain control of your e-mail account and help protect it from being compromised in the future:

- Contact your e-mail provider and inform them that your e-mail was hacked.
  If you can't access the e-mail account because your password has been changed, notify them immediately and follow their instructions for recovering a hacked account.
- Change your password.
  Use strong passwords that contain 8–10 characters and use a combination of letters, numbers, punctuation and symbols.
- Change your security questions.
  Many e-mail accounts use security questions to help you access your account when you forget your login information or to confirm your identity if you're accessing the e-mail account from an unfamiliar computer. If the hacker knows the answers to your security questions, he or she may be able to regain access to your e-mail account, so pick different questions with answers unrelated to your previous security questions.
- Consider adding a cell phone number to your account.
  If you add a cell phone number and choose a two-step login authentication process, you will receive a text containing a numeric code you need to enter in addition to your password. If you already have a phone number attached to your e-mail account, check that this number wasn't changed.
- Check that your recovery e-mail address wasn't changed.
  The recovery e-mail address is used to reset or regain access to your login ID/password. If this was changed, your e-mail account might be compromised again, so be sure to switch it to an e-mail only you have access to.
- Check the "forwards."
  Check that your e-mail account hasn't been set up to forward e-mails to the hacker. If you're not sure where to find this e-mail option, contact your e-mail service provider or check their website for FAQs about setting up forwards or automatic responses.
- Change your passwords on any associated e-mail accounts.
  The hacker might attempt to reset your login information for sites that use the compromised e-mail address as the primary login identifier.

Two-step authentication

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

Check out the tips on page 5 for more tips on how to set up a strong password.