ABCs of Staying Safe Online *(...and on the telephone)*

Using email and surfing the internet opens up so many possibilities: connection to friends and family, convenience of shopping and banking online, and a world of information at your fingertips. But our online lives may also bring exposure to fraudsters. At TechMoxie, we believe that a little information goes a long way. Learning how fraudsters operate and what they are looking for will help you navigate online as safely as possible.

Our ABCs cover the *most common* scams and offer tips on how to avoid them.

A. Understand What Fraudsters May Want...

To defraud you of money	Scams change quickly, but we can say with certainty that there will always be people trying to part us from our money. Recently we have seen attempts to sell fraudulent computer services by claiming your computer has a “dangerous virus” or needs “cleaning”. Phone callers may claim that you owe money to the IRS or pretend to be a relative in trouble.
Your personal information	There is a black market for personal data. A credit card number becomes more valuable if it includes data such as your zip code and a card’s security code.
To infect your computer	Fraudsters might simply be to put advertising “pop ups” on your computer, or something more harmful like a virus, also known as malware.

B. Know How Fraudsters Reach Potential Victims

Email	Known as “phishing” (phony + fishing), sending fake emails is a favorite way for fraudsters to find victims as it is easy to copy the logo of a well known business to make an email that looks like it came from Wells Fargo, FedEx, Facebook, or even a friend. All email accounts now have filters that attempt to put fraudulent emails in special “junk” or “spam” folders. But some fraudulent email may slip into your inbox.
Pop Ups	These are ads that “pop up” on your screen while using the internet. Most are just annoying - not criminal. But occasionally they freeze your computer with fake warnings that your system is damaged or needs “cleaning”.
Fake Websites	Fraudsters will create fake websites that have similar URLs as real ones hoping to catch people that misspell the website. e.g., YuTube.com instead of Youtube.com.
Telephone	Many fraudsters try to reach victims by telephone. The scams change over time, but recent examples include phone calls that claim to be from the IRS, local police and even people posing as a relative in trouble.

C. Tips to Help You Stay Safe

1	**Think before you click!**	Assume that clickable links in email are fraudulent until you can assure yourself otherwise. Follow our tips to help you stay safe.
2	**Fraudsters use the names and real logos of companies**	Emails may look like they were sent by companies you do business with. The scams change, but we have seen fraudsters send convincing emails pretending to be: • Google, Yahoo or AOL saying that you have missing or compromised mail. • Fed Ex, Amazon, or UPS saying a package was delivered. • A bank asking you to update account info.
3	**Emails may look like they came from a friend**	Fraudsters can make an email look like it came from a friend's account - even if that account wasn't actually hacked. **Examples:** • The email says that your friend or family member is out of the country and needs you to send them money due to an emergency. • The email may have no message but a link to a website. • Or the email may have a link and very short (and tempting!) message such as: "*Hey, you have to see this*" or "*Check out these photos!"* If in doubt, call to confirm that your friend or family member really sent it.
4	**Be familiar with common email scams**	Remember, fraudsters are often after your personal data or money. So be on the look out for emails that: • ask you to verify or update account information. • offer you a 'free' gift card or deep discount on products. • tempt you to click on links to 'family photos'.
5	**Before clicking, ask yourself these questions**	• Are you expecting an email from the sender? • Does the email have enough detail to convince you that it is legit? e.g., "here is a link to those photos of Mary and Sally from our dinner in DC last week" is pretty specific. But an email that says "Hey, here are the pictures" could be from anyone. • If the email appears to be from a friend, call the friend to confirm that they sent you the email.
6	**If possible, don't click, go to web browser instead.**	Even if you think a link in an email is legitimate, don't click but instead go to the website directly via your browser. For example, if you get an email regarding a bank account, don't click in the email. Go to your browser and access the website directly.

C. Tips to Help You Stay Safe

7	**Know what to do with “bad” emails**	• Don’t click on any links in the email. • Don’t forward the email. • Delete the email. • Emails in your junk or spam folder generally are automatically deleted in 30 days.
8	**If your computer has a pop up or message you can’t close or remove**	• Shut the power to your computer by pressing and holding the power button or simply unplug it. • Turn the computer back on. • When your internet browser (e.g., Chrome or Explorer) reopens, it may have a message like *“your last session stopped unexpectedly would you like to restore it?”* Click *‘No”*
9	**Watch for Telephone Scams**	The scams change, but often follow these themes: • Caller claims to be a relative in trouble (e.g., a grandchild). • Caller says that you have a gift waiting but a credit card is needed to cover for delivery charges. • Caller claiming to be from the IRS, police, court, or other government agency.
10	**Keep your software up to date**	Companies like Microsoft, Apple, and Adobe constantly look for vulnerabilities that fraudsters can take advantage of. They issue software updates to fix problems. Some computers may be set to automatically update, but others may require you to take specific action. And be sure to keep smartphones/tablets up to date.
11	**Beware of pop up alerts that your computer needs to be “cleaned” or “repaired”**	Don’t believe anyone that tells you that computers need to be cleaned or serviced to make them run well unless *you* are experiencing a problem. Such a message is likely coming from a fraudster looking for large fees to “fix” your computer. If you can’t close the message, follow steps in tip #8.
12	**Use Google search to reach your website**	Use Google search to get to websites rather than trying to type precise web addresses into your browser. Why? Because a typo can land you on a fake website. Google corrects typos automatically so typing “WelsFargo” will get you safely to “WellsFargo”.
13	**A note about passwords...**	Most online accounts now require lengthy and unique passwords. It is recommended that you have a unique passwords for each site/account. However, users have to balance this with the challenge of remembering so many passwords. Many web browsers (e.g., Chrome) will remember your password for you if you choose, but not guaranteed to be risk free either. Spreadsheets work well for some. And another option is an online password manager, such as LastPass. Users have to decide what is right for them.

What to do if you have been defrauded?

Unfortunately, it isn't practical for law enforcement to respond to every instance of a suspicious email. But know that the email providers (e.g., Google) and federal and local enforcement agencies (e.g., FBI and FTC) are working to keep to make it harder for fraudsters to reaching you.

If you have been a victim of fraud, start by reporting it to you your local police. Many police departments now have special divisions that handle financial and cyber-crimes. The first step is to call their non-emergency number to start the reporting process.

If you think you might be a victim of identify theft, file a fraud alert with Equifax (the credit reporting bureau). Once filed, Equifax will share the alert with other credit bureaus. From Equifax's website:

> "A fraud alert is a notice or flag added to your credit file. This notice or flag alerts recipients of your credit file that you may be a victim of fraud, or that you suspect you may be a victim of fraud, including identity theft. It also requires that they follow certain procedures to verify your identity in connection with requests for new credit accounts, increasing credit on an existing account, or issuance of a new card on an existing account. There are two types of fraud alerts: an initial fraud alert that lasts for 90 days, and an extended fraud alert that lasts for 7 years.

The extended fraud alert requires that you have a police report or other evidence of identity theft, but the initial fraud alert my be filed quickly and easily online.

If fraudulent or even questionable fees were charged to your credit card, report this immediately to your credit card company. They are obligated to put a hold on the charges to give you time to complete a report. With a little perseverance, you may succeed in getting the charges reversed.

If you think that your email or other account has been hacked, change your password. If you become aware that friends are getting fraudulent emails from you, send an email out to your contacts letting them know to ignore the "bad" email.

About TechMoxie

We help grown ups *with technology with both instruction and support. We offer in-home instruction and support, classes, and community talks.*

We offer a free community talk on Staying Safe Online. Contact us for more info!

202.642.5520 or email info@tech-moxie.com