Tamarind
FINANCIAL PLANNING

FINANCIAL PLANNING
FOR LIFE'S BIG ADVENTURES

Cybersecurity 101: Online Safety Tips

STAYING SAFE ONLINE

The internet has become an increasingly essential part of our daily lives. We have come to appreciate and rely on the products and services we access online for both our personal and work lives.

It's more crucial than ever to be aware of our vulnerabilities online and take responsibility for our internet safety.

What precautions can you take to protect your systems and personal information to mitigate identity theft and potential financial loss? See below:

QUICK TIPS TO STAY OUT OF TROUBLE ONLINE

1. Don't click on links and attachments in emails

- Unless very sure they are legitimate
- Beware of all messages, even from friends and known persons
  Some hacker emails look authentic and come from people you know (as they may have been hacked)

2. Don't send personal information via email

- Pick up the phone or use secure download/upload

3. Use password managers

4. Do the 2 step

- Always use two factor authentication when available

5. Verify callers

- If you get a call that seems suspicious, hang up and call back the phone number on the website
- Even if it doesn't seem suspicious, if it comes from a critical institution like your bank and asks for personal and/or account details, just be safe -- hang up and call back

6. Keep credit frozen and locked

- Unfreeze only if needed & for short periods (for example, 3 days or whatever is absolutely necessary)

WWW.TAMARINDFINANCIAL.COM

EMILIE R. GOLDMAN, CFA, CFP®
emilie@tamarindfinancial.com
ARIADNE HORSTMAN, CFP®, RLP®
ariadne@tamarindfinancial.com

QUICK TIPS TO STAY OUT OF TROUBLE ONLINE, *continued*

7. **Don't put off computer/software updates**
    - Security patches are developed rapidly as hackers discover vulnerabilities.
    - Take advantage and update as soon as offered

8. **Frequently take time to delete files from the Downloads folder on your computer**

9. **Connect securely**
    - When out of the office, use a Wi-Fi hotspot from your phone or a secure VPN to connect

10. **Use a long passphrase**
    - Such as: Ihate2dothedishes
    - It's more secure the longer it is

11. **Empty your laptop recycle bin**

12. **Cover Up!**
    - Keeping your laptop camera under wraps is important
    - Most laptops come with a camera cover these days that you can close manually

HOW ARE WE VULNERABLE?

Four main types make up the many threats we are exposed to when we use the internet:

Ransomware
If you do not carefully watch the websites you are visiting, you could get attacked by ransomware that could lock or encrypt the data on your computer. It's called ransomware because a ransom is demanded to release your locked data.

Identity Theft
Information you put online such as your personal details and photos can be used to steal your identity.

Phishing Emails
Emails are used by con artists, fraudsters, and social engineers to trick you into providing sensitive information.

Malware
Software that is written with the intent of damaging your devices and stealing your data.

EMILIE R. GOLDMAN, CFA, CFP®
ARIADNE HORSTMAN, CFP®, RLP®
emilie@tamarindfinancial.com
ariadne@tamarindfinancial.com

WHAT CAN YOU DO TO PROTECT YOUR PERSONAL INFORMATION?

Follow these tips to keep your information safe:

Passwords

- Never share or reveal your passwords.
- Use strong passwords, the longer, the better. A pass phrase is easier to remember if the website does not require you to use special characters.
- Change passwords every 90 days and have a different one for each online account
- A password manager can help you generate complex passwords and store them in an encrypted manner.
- Two-factor authentication on website and phone logins adds an extra layer of security in addition to entering your password.

Emails / Phone Calls

- Watch out for links in emails that may take you to a fake website or attachments that could download malicious code to your computer/network. Visit a company's website by using their official address, not the link you may have been sent. Find their email address or phone number and contact them directly.
- When the message comes from someone you know or think you know, you are more likely to trust the message. Verify the identity of the caller or the sender of emails that ask you to do something.
- Analyze the information you're being asked to provide and how – check for reasonableness.
- Be wary of emails, phone calls or other messages when they convey a sense of urgency or high pressure asking you to provide sensitive personal information.

Social Media

- Reduce personal details on your social media to the bare minimum.
- Apply privacy settings to your social media accounts to control who can see your information.

Credit

- Freeze your credit with major credit agencies: Equifax, Experian, and TransUnion. You can visit their websites to freeze and unfreeze your credit. Temporarily unfreeze your credit as needed, for example, when applying for a loan or a credit card.

Websites

- Confirm the URL for websites you visit start with https. The 's' stands for secure.
- Look for a lock icon next to the URL, and check that the full URL is legitimate.
- Avoid entering your credit card information on an unfamiliar website.

WWW.TAMARINDFINANCIAL.COM

EMILIE R. GOLDMAN, CFA, CFP®
emilie@tamarindfinancial.com
ARIADNE HORSTMAN, CFP®, RLP®
ariadne@tamarindfinancial.com

Computer

- Install anti-virus software, anti-spyware and latest security patches on your computer/devices. Make sure they are from reputable vendors.
- Make sure your computer has a login password to keep others out.
- Encrypt your laptop (you may need to ask your tech person to help)

Wi-Fi

- Ensure your home Wi-Fi network is secure and uses a strong password.
- Do not send/view sensitive information over public Wi-Fi networks. If you need to use public Wi-Fi, use a secure VPN or try connecting to your phone hotspot.

WORKING FROM HOME

If you are working from home, as many of us are these days, there are additional precautions you can take to keep sensitive data safe.

Encrypted Hard Drive

Encrypt your desktop, laptop, external hard drives and any other devices you use for work.

File Sharing

To share files with your colleagues and clients, use a secure filing sharing system instead of transmitting files via email.

Webcam

When you are not using your camera for a video meeting, make sure to cover the webcam. Hackers have been known to remote access into webcams.

Downloads

When downloading client files from emails or other software, make sure you save the file in a secure place and delete the downloaded copy from the downloads folder.

Device Remote Access

Make sure you can shut down your computer/phone remotely. Most devices allow you to do this — it is helpful to have in case your device gets stolen or lost.

EMILIE R. GOLDMAN, CFA, CFP®
emilie@tamarindfinancial.com
ARIADNE HORSTMAN, CFP®, RLP®
ariadne@tamarindfinancial.com