B.O.S.S.
RETIREMENT SOLUTIONS & ADVISORS

INVESTOR PROTECTION CHECKLIST

The educational checklist presented below is designed to help you take appropriate action to better protect you and your family from the risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

1. MANAGE YOUR DEVICES

ACTIONS TO CONSIDER

□ Install the most up-to-date anti-virus and anti-spyware programs on all devices, and update these software programs as they become available. These programs run regularly rather than just running periodic scans, which may not provide maximum protection to your device.

□ Access sensitive data only through a secure location or device. Never access confidential personal data via a public computer.

□ Set up a separate computer your children can use for games and other online activities.

□ Keep software patched. Many updates are made to resolve recently identified security risks.

□ Do not install pirated software. It often contains security exploits. Do frequent backups in case of ransomware attacks.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

2. SURF THE WEB SAFELY

ACTIONS TO CONSIDER

□ Do not connect to the internet via unsecured or unknown wireless networks, such as those in public locations. These networks may lack virus protection, are highly susceptible to attacks and should never be used to access confidential personal data.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

3. PROTECT ALL PASSWORDS

ACTIONS TO CONSIDER

□ Consider using a password manager program. These programs help maintain complicated passwords but can be exploited if the vendor has a breach.

□ Use a personalized custom identifier for financial accounts you access online.

□ Never use your Social Security number in any part of your login activity.

□ Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships.

□ Avoid storing passwords in email folders.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

4. SAFEGUARD YOUR FINANCIAL ACCOUNTS

ACTIONS TO CONSIDER

□ Lock down personal credit reports with Experian, TransUnion and Equifax.

□ Proactively enroll in an identity theft protection service to protect personal data.

□ Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held.

□ Never send account information or personally identifiable information over email, chat or any other unsecured channel.

□ Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the website's URL into the browser yourself.

□ Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

5. PROTECT INFORMATION ON SOCIAL MEDIA

ACTIONS TO CONSIDER

□ Limit the amount of personal information you post on social networking sites. Never post your Social Security number. Consider keeping your birthdate, home address and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays or the loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

6. PROTECT YOUR EMAIL ACCOUNTS

ACTIONS TO CONSIDER

□ Delete any emails that include detailed financial information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account.

□ Use secure data storage programs to archive critical data and documents.

□ Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those warning that your computer is infected with a virus requesting that you take immediate action.

□ Establish separate email accounts for personal correspondence and financial transactions.

CHECK WHEN COMPLETED

□ I've reviewed and understand all the items above.

□ I've taken action for those that apply to my situation.

HOW CRIMINALS ACCESS PERSONAL INFORMATION

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the Investor Protection Checklist are intended to help you and your family better protect yourselves against such activity.

MALWARE. Using malicious software, criminals gain access to private computer systems (e.g., a home computer) and gather sensitive personal information, such as Social Security numbers, account numbers, passwords and more.

How it works

While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email.

PHISHING. In this ruse, criminals attempt to acquire sensitive personal information via email. Phishing is one of the most common tactics observed in the financial services industry.

How it works

Masked as an entity with which the victim may already have a financial relationship (e.g., a bank, credit card company, brokerage company or other financial services firm), the criminals request sensitive personal data from unwitting recipients.

SOCIAL ENGINEERING. Via social media and other electronic media, criminals gain the trust of victims over time, manipulating them into exposing confidential information.

How it works

Typically, these scammers leverage something they know about the person, such as their address or phone number, to gain their confidence and get them to provide more personal information, which can be used to assist the criminals in committing fraud. Social engineering has increased dramatically, and, many times, fraudsters are contacting investors by phone.

NETWORK SECURITY. Attacks against home and business networks are typically not personal in nature and can occur on any type of network—big or small, home or business. If a network connects to the internet, it's inherently more vulnerable and susceptible to outside threats.

How it works

Many internet-enabled products come preconfigured with factory-issued settings, including default usernames, passwords or security settings. Many people leave these unchanged, creating opportunities for malicious cyber actors to gain unauthorized access to information, install malicious software (malware) and cause other problems.

Although cases of cyber fraud continue to worsen worldwide, B.O.S.S. Retirement Solutions & Advisors goes above and beyond to keep you and your family's data protected.

Here's how:

EMAIL HOSTING, INCLUDING SPAM PROTECTION

Real-time email scans filter our outbound emails, protecting us from incoming spam and store received emails automatically.

MANAGED SECURITY SERVICES

Managed security services run anti-virus and anti-spam programs to safeguard us from vulnerability.

NETWORK PERFORMANCE MONITORING

Network performance is monitored around the clock to ensure our devices and infrastructure continue functioning properly.

ENDPOINT ANTIVIRUS

Anti-virus scanning prevents the spread of malicious emails and saves us from losing files if a server should ever go offline.

IMAGE-BASED BACKUP/DISASTER RECOVERY

Proactive disaster recovery programs back up all our data and information in the event of an emergency.