Prevent Cyber Crime

FINANCIAL PLANNING

ALLODIUM®
INVESTMENT CONSULTANTS

Cyber crime is a serious threat and constant vigilance is key. This checklist summarizes common cyber crime tactics, along with prevention tips and best practices. Methods used to compromise a victim's identity or login credentials—such as malware, phishing and social engineering—are increasingly sophisticated and difficult to spot. A fraudster's goal is to access your account and assets to obtain or sell information. Following best practices and applying caution when sharing information or executing transactions can make a big difference.

WHAT YOU CAN DO TO PROTECT YOUR INFORMATION AND ACCOUNTS	
Keep your financial advisor informed regarding changes to your personal information.	✓
Freeze your credit file with each of the three credit bureaus (Experian, Equifax and Transunion) to protect against identity theft.	
Check your credit report regularly at www.annualcreditreport.com for unauthorized activity.	
Be on the lookout for someone using your Social Security number to claim a fraudulent tax refund or other tax-related identity theft. Contact the Internal Revenue Service at **www.irs.gov** if you believe you are the victim of tax-related identity theft.	
Be aware of suspicious phone calls, emails and texts asking you to send money or disclose personal information. If a service rep calls you, hang up and call back using a known phone number. Never share sensitive information or conduct business via email.	
Beware of phishing and malicious links. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or install malware. Check your email and account statements regularly for suspicious activity.	
Never enter confidential information in public areas. Assume someone is always watching. Consider using a locked mailbox.	
EXERCISE CAUTION WHEN MOVING YOUR MONEY	
Leverage your custodian's electronic authorization tool to verify requests.	
Review and verbally confirm all disbursement request details thoroughly before providing your approval.	
ADHERE TO STRONG PASSWORD PRINCIPLES	
Don't use personal information as part of your login ID or password and don't share login credentials.	
Create a unique, complex password for each website; change it every six months. Consider using a password manager.	
MAINTAIN UPDATED TECHNOLOGY	
Keep your web browser, operating system, antivirus and anti-spyware updated; activate the firewall.	
Do not use free or found USB devices. They may be infected with malware.	
Check security settings on your applications and web browser. Make sure they're strong. Turn off Bluetooth when it's not needed.	
Dispose of old hardware safely by performing a factory reset or removing and destroying all storage data devices.	
USE CAUTION ON WEBSITES AND SOCIAL MEDIA	
Do not visit websites you don't know, (e.g., advertised on pop-up ads and banners).	
Log out completely to terminate access when exiting all websites.	
Don't use public computers or free Wi-Fi. Use a personal Wi-Fi hotspot or a Virtual Private Network (VPN).	
Hover over questionable links to reveal the URL before clicking. Secure websites start with "https," not "http."	
Be cautious when accepting "friend" requests on social media, liking posts or following links.	
Limit sharing information on social media sites. Assume fraudsters can see everything, even if you have safeguards.	
Consider what you're disclosing before sharing or posting your résumé.	
WHAT TO DO IF YOU SUSPECT A BREACH	
Call your financial advisor or your custodian immediately so that they can watch for suspicious activity.	

Learn More: Visit these sites for more information and best practices.

- **StaySafeOnline.org:** Review the STOP. THINK. CONNECT™ cybersecurity educational campaign.
- **OnGuardOnline.gov:** Focused on online security for kids, it includes a blog on current cyber trends.
- FDIC Consumer Assistance & Information, **https://www.fdic.gov/consumers/assistance/index.html.**
- FBI Scams and Safety provides additional tips, **https://www.fbi.gov/scams-and-safety.**