# CYBER SECURITY CHECKLIST

Cyber criminals exploit our increasing reliance on technology. 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 obtain information to access to your account and assets or sell your information for this purpose. Following best practices and applying caution when sharing information or executing transactions makes a big difference.

## HOW WE CAN WORK TOGETHER TO PROTECT YOUR INFORMATION AND ASSETS

- **Keep us informed** regarding changes to your personal information.
- **Expect us to call you to confirm email requests** to move money, trade, or change account information.
- **Notify us immediately** if you suspect a breach.

## WHAT YOU CAN DO

□ Be aware of suspicious phone calls, emails, and texts asking you to send money or disclose personal information.

□ Never share sensitive information or conduct business via email, as accounts are often compromised.

□ Beware of phishing and malicious links. Urgent-sounding, legitimate-looking emails are intended to tempt you to accidentally disclose personal information or install malware.

□ Don't open links or attachments from unknown sources.

□ Check your email and account statements regularly for suspicious activity.

## EXERCISE CAUTION WHEN MOVING MONEY

□ Review and verbally confirm all disbursement request details thoroughly before providing your approval, especially when sending funds to another country. Never trust wire instructions received via email.

## 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 to simplify this process.

## MAINTAIN UPDATED TECHNOLOGY

□ Keep your web browser, operating system, antivirus, and anti-spyware updated, and activate the firewall.

□ Do not use free/found USB devices. They may be infected with malware.

□ Check security settings on your applications and web browser. Make sure they're strong.

□ 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.

## 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.