ROCKLAND TRUST

Where Each Relationship Matters®

Common threats and how to avoid them

Threat	How it works	How access is gained	How to protect yourself
Spoofing	• A caller manipulates the information shown on your caller ID to hide their true identity.	• By displaying a phone number from a legitimate company on your caller ID, it increases the likelihood that you will answer the call. Having gained your trust, the caller will push you for personal information.	• Don't answer calls from unknown numbers. If you do answer, remember that you will never have to give money to obtain a refund or to fix an issue. • Do not engage in casual conversation, even if it feels harmless. The more you talk, the more information you are giving the scammer. • Talk to your mobile carrier about blocking tools and apps to block unwanted calls. • Remember to use caution if you are being pressured for information during the call. • If you are unsure if the call is legitimate, hang up and call a known number from their verified website. Do NOT call a number they give you or the one they called you from.
Malware (Viruses, worms, trojan horses, spyware, adware)	• Cyber criminals entice you to click on an email attachment or a photo or video from a social media site.	• Clicking on an infected document, video, or photo can install software that allows thieves to access user names, passwords, account numbers, social security numbers, and other sensitive data. Malware can be found on legitimate social networking sites. Sometimes, malware is disguised as genuine software and may appear to come from an official site.	• Never click on links or open attachments within an email if you don't recognize the sender. Click on the sender's email address to reveal the actual URL. Sometimes the URL may look like a trusted sender, but is missing a letter to trick you. • Install up-to-date security software on all your devices, including antivirus, anti-spyware, anti-phishing, and a firewall. • Read software agreements to understand exactly what applications are being installed. • Keep your software licenses current. • Set your operating system (e.g., Windows) to update automatically. • Do not conduct any online banking activity if you think your computer or phone may be infected with malware. Have your device thoroughly checked by a security specialist.
Ransomware	• Malicious software freezes your computer or mobile device until a sum of money is paid.	• Clicking on a phishing email, advertisement or popup window, or by downloading software.	• Enable popup blockers. Depending on your browser, this option may appear under *privacy and security* or *preferences*. • Download software only from sites you know and trust. • Backup files offline.
Mobile device fraud	• Mobile devices are particularly vulnerable to malware that can steal banking data.	• By downloading apps from disreputable places, visiting sketchy websites and pages, clicking links from unknown sources, and more.	• Lock your phone when not in use and always keep it with you. • Don't conduct online banking over public wireless networks. • Don't send sensitive information if you can't verify that a Wi-Fi network is secure. • Research apps before you download them. Beware of fake apps that mimic real ones. Check the validity of an app on your phone's app store. It should be developed by the company itself, and have a lot of ratings and reviews from other users. • Do not store confidential information on a mobile device unless it is encrypted.

Report suspected bank fraud immediately! Contact us at 508.732.7072 or Customer.Support@RocklandTrust.com

ROCKLAND TRUST

Where Each Relationship Matters®

Cyber threats and how to avoid them (continued)

Threat	How it works	How access is gained	How to protect yourself
ID Theft	• Fraudsters steal your information.	• Leaving your computer unattended when logged in to online banking. • "Dumpster diving", a practice where fraudsters steal your information from the trash.	• Use a secure browser and a trusted computer. • Log off your online banking session when finished. • Set up security alerts in online banking. • If you still receive paper statements, make sure you receive them on schedule. Consider switching to eStatements. • Check your statements and transaction history often to ensure the accuracy of your accounts. • Don't include sensitive information in email. • Be suspicious of any emails or phone calls asking for personal information and emails with misspellings or bad grammar. • Be selective when providing your email address.
Password exposure	• A weak password can allow hackers and malicious software to gain access to your accounts.	• Cyber criminals can steal passwords by using malware (such as keystroke monitoring), trial and error sessions, hacking into databases, and simply by looking over your shoulder.	• Choose a password only you would know. Don't pick a word from the dictionary. Use a combination of at least eight letters, numbers, and symbols. • Change your passwords regularly. • Use different passwords for all of your online accounts. If you use the same password everywhere and it is ever stolen, you could lose access to all of your accounts at once. • Log off when you're finished using websites that require a user ID and password. • Make sure the "remember me" function is not enabled when using a public computer.
Social engineering	• The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.	• Imposters call or email you posing as a bank employee, the IRS, or some other authority.	• Remember, Rockland Trust will never reach out to you and ask for personal information, online banking credentials, or your PIN on the phone or in an email. • The IRS, Homeland Security, credit card company, or any legitimate company will never email or call you demanding immediate payment without having first mailed a bill — nor will they ask for a credit or debit card number via email or phone. • The American Banking Association provides tips and tools on what information banks do and don't ask for at **BanksNeverAskThat.com**

Report suspected bank fraud immediately! Contact us at 508.732.7072 or Customer.Support@RocklandTrust.com