ltr ProEquities
listen, think, respond

# ONLINE SECURITY DISCLOSURE

## Risks of Using Electronic Communications

Technology has made it easy for hackers to cast a very broad net in their quest to obtain confidential information instantaneously and cheaply. With the press of a button, a hacker can launch 100,000 emails to as many potential “marks” containing malicious email or text, all designed to provide access to the information on your computer, mobile device, and related online accounts. This disclosure provides basic steps you can take to enhance your cyber security.

## Email Communications: Be Alert to Phishing Attempts

Email is an efficient form of communication; however, it carries particular risks. Utilize an email service provider that features encryption. Send personal information through known and trusted sites only; and, if you manage any financial accounts online, check them regularly for any unusual activity.

Beware of attempts to "phish" your information. These are often in the form of urgent-sounding emails where you might be encouraged to click on a link in order to update personal information. Even clicking on the link could potentially take you to a malicious website where malware could infect your computer. We strongly recommend that you not click on suspicious links. Instead, navigate directly to a known web address.

Do not open emails from senders you do not recognize. Never open attachments or click on embedded links unless you are sure of their authenticity. This is true even if the email appears to come from someone you know. Remember, it is very common for hackers to learn the email addresses of individuals in your network and send emails that appear to come from similar addresses (e.g., John.Smith@proequitiesBD.com).

## Keep Your Equipment Updated

Technology changes quickly. Keep your computer's antivirus and firewall software current. Ensure your computers are encrypted. Auto-install essential operating system updates. Lock your computer and mobile devices when not in use.

## Create Strong Passwords and PINs

Hackers can crack a six-letter password in minutes. By adding uppercase letters, symbols, and numbers, the time it would take to crack your passcode increases exponentially. Avoid the most common passwords, like “123456” or “password.” Also avoid using your children's names, your pet's name, the last four digits of your Social Security number, or any other item of information that may be readily accessible by others.

Ensure each password is at least eight characters long. Instead of using a word like “bostonian” as your password, substitute numbers and symbols for lower case letters like “B0st0n!an04”.

Memorize your passwords and PINs, and not write them down. Do not share your passwords and PINs with anyone, even if someone asks. *Note: Your financial institutions will not ask you for this information.* Finally, change your passwords and PINs regularly, especially if you suspect that someone may have knowledge of them.

Consider using more than one method of authentication, such as a password and a text code or a one-time password and challenge question. Some websites offer an authorization code, which is a one-time number sent via email or text when you log in.

**Mobile Device Security**

Mobile devices, including phones and tablets, are essentially small computers and vulnerable to viruses and malware. Update your mobile device operating system regularly and keep the following tips in mind:

- For maximum security, download the mobile application directly from your financial institution’s website.
- Guard personal information on your phone or tablet by using strong passcodes and a short screen lock period (e.g., one minute).
- Use caution when browsing websites, downloading applications, performing financial transactions, and sharing personal information or location. Avoid using unsecured public Wi-Fi hot spots, as they are susceptible to security breaches. Investigate the use of a personal VPN to ensure secure connections when away from a secure network. Never accept software updates when using public Wi-Fi.
- Do not respond to suspicious texting, calls, or voicemails. Requests for personal information or a call for immediate action are almost always scams.