Richton Bank & Trust Co.

Partnering for Online Security

Online banking has grown rapidly into a major new way to bank. Some surveys show that more people prefer to bank online than in the traditional ways. This phenomenal growth has been accompanied by increases in the safety and security measures undertaken by banks and their customers. Cyber-criminals are always looking for new ways to electronically break into the bank and steal your money. Safe online banking depends on continuing and strengthening this partnership for safe online banking:

✦ BANKS INVEST SUBSTANTIALLY IN SECURITY✦

Lawmakers, regulators, and the banking industry have forged substantive standards for safeguarding customers' personal information. Uniform examination procedures are in place to monitor and enforce these standards, and bank examiners regularly go on-site to assess how bank security measures are being implemented, understanding that each bank has a different menu of products and services, and therefore differing security requirements. Some of the areas they look at include:

- Access controls ensuring customer information can be accessed only by authorized persons, including use of multi-factor authentication when warranted.
- Physical restrictions at computer facilities that permit access to authorized persons only.
- Data encryption of electronically transmitted and stored customer information.
- Modification procedures to ensure that changes are consistent with the approved security program.
- Dual control procedures, segregation of duties, and employee background checks.
- Monitoring procedures to detect actual and attempted intrusions into customer information.
- Response programs specifying actions to be taken by specific individuals when the institution suspects unauthorized access.
- Environmental hazard protections against physical damage or technology failures.

✦ BANKS PARTNER WITH YOU, THE CUSTOMER✦

Your bank has security measures to protect your account information, but they cannot be effective without your help and cooperation. Many account hijacking attempts come as a result of hacking into individual user accounts, and from there electronically breaking into the bank using your information and security codes. Some common sense and easily implemented precautions can help you safeguard your personal information:

- Strong Passwords—Experts advise a combination of letters and numbers and advise against using easily guessed passwords such as birthdays or home addresses.
- Anti-Virus Protections—Make sure the anti-virus software on your computer is current and scans your email as it is received.
- Email Safety—Email is generally not encrypted so be wary of sending any sensitive information such as account numbers or other personal information in this way.
- Sign Off and Log Out—Always log off by following the bank's secured area exit procedures. Understanding how criminals try to trap you is your first line of defense:

- PHISHING—This is the criminal attempt to steal your personal information through fraudulent emails or smart-phone texts. They are often very believable, luring the victim to a site that asks them to provide (or "verify") personal financial details such as account numbers and social security numbers. A variation is called Spear Phishing, which are electronic messages that appear to come especially to victims from their employer, usually a large corporation.
- Cyber-security experts often term the mobile phone version of phishing, Smishing, playing off the SMS, or Short Message Service terminology used in text messaging. Remember: your bank will not send emails asking for your personal information—they already have it.
- CARD SKIMMING—This is a criminal's attempt to gain a victim's personal information by tampering with ATM machines. Fraudsters set up a device that can capture magnetic stripe and keypad information, such as PINs and account numbers. Using ATMs you know and trust—as well as examining the machine closely—can help thwart this type of theft.
- SPYWARE—This is the term used for criminal software that a victim unknowingly loads on a personal computer. Once there, the spyware collects personal information and sends it to the criminal. Up-to-date security software is the best defense. HELPFUL HINT: Cyber-criminals often prey on those who are most vulnerable, such as senior citizens or young adults, who may not be as aware of the technical aspects of the threats. Make sure you alert any friends or family members who might be in this category. They will appreciate it!

✦ONLINE & MOBILE THREATS✦

Cyber-fraudsters want to earn their money the easy way—by stealing yours.

- Do not Get Phished—Crooks are always trying to get your personal information, and they employ some ingenious methods. Do not respond to any unusual email requests for personal information— when you opened your bank accounts you already gave it. When in doubt, call your bank.
- Monitor Your Accounts—When you check your accounts regularly, you can let your bank know immediately if you encounter anything that does not seem right. HELPFUL HINT: Studies show that those who monitor their accounts online often detect fraud earlier than those who rely solely on paper statements.

✦ FREE CREDIT REPORTS✦

YOUR BEST TOOL

When it comes to guarding against cyber-fraud, one of the most important tools at your disposal is your credit report. It details all your credit transaction accounts and will be the first place that unusual charges or entirely new accounts will appear. And you can monitor your report for FREE. Since Federal law permits consumers to obtain a free report annually from each of the three major credit reporting agencies, cyber-security experts advise that you to get a free report from a different agency every four months. Doing so will allow you to monitor your personal online security all year long.

TO ORDER YOUR FREE CREDIT REPORT, GO TO THE ONLY AUTHORIZED SOURCE:

www.annualcreditreport.com