YOUR SECURITY MATTERS

At Iroquois Farmers State Bank our top priority is the security and privacy of your financial information. We maintain physical, electronic, and procedural safeguards that comply with federal standards to protect your personal information. Iroquois Farmers State Bank continually monitors and reviews all of its security protection measures. As new technology or improved practices become available, we will adopt those that we believe may improve the security of your confidential financial information.

Iroquois Farmers State Bank also wants to help you protect yourself against crimes targeted against consumers such as identity theft and E-mail "Phishing." The following information is provided to help protect you from becoming a victim and some steps to take if you believe that you have been a victim of identity theft.

Identity Theft

Identity theft occurs when someone illegally obtains your personal information, such as your social security number, credit card number, bank account number, or other identification, and uses it to open accounts or initiate transactions in your name.

E-mail and Website Fraud (Phishing)

One of the most common types of e-mail fraud is sending a phony e-mail message that directs the recipient to a fraudulent website. These e-mails can look very convincing. There are some common features among many of these types of e-mail.

- Urgent appeal. The message may threaten some consequence if you do not respond.
- Request for Information. There may be a request to update or validate certain personal information.
- Typos and errors. Often the message is poorly written or has spelling errors within the message.

How to Prevent Being Phished

- Don't reply to any suspect or suspicious e-mail, even if it seems urgent.
- Don't click on links inside of e-mail.
- Don't call telephone numbers from e-mail. Instead, call the number on the company website, phone book, statement, or back of a credit/debit card.

Security Tips – Web browsing and Mobile Phones

Technology has become increasingly sophisticated. Make sure your security measures can keep up by reviewing your web browsing and mobile phone practices. You never know what actions might leave you vulnerable to identity theft. Don't know where to begin? We can help. There's only one you, and these tips will help keep it that way!

- Secure your computer. Ensure that you have anti-virus and anti-spyware software and a personal firewall installed on your computer. Many of these products are available that will help you protect information on your computer or while using your computer.
- Do not reply to, or click on, a link in an e-mail that warns you, with little notice or prior legitimate expectation, that an account of yours will be shut down unless you confirm billing or other account information. Instead, contact the company cited in the e-mail by using a telephone number or other form of communication that you are sure is genuine.
- If you install apps and features containing sensitive information, like bank accounts, credit cards, healthcare records, and tax statements, always update to the latest operating software and maintain strong passwords.
- Avoid mobile apps that require permissions and insist on requiring unnecessary personal information. Sensitive data usually isn't required but, when it is, make sure the app is verified and user-approved. You can do some research by scanning user reviews online and searching for proof of authenticity.
- If you have bank apps on your phone, always log out of these accounts after using them. It's tedious, but it's worth it.
- It's always exciting to find free Wi-Fi, but, sadly, it almost always means the connection is unsecured. Be careful with public networks, especially when accessing information like banking and credit card details.
- Those small cellphone screens may make it hard to detect an illegitimate email. That's all the more reason to slow down and evaluate any message you receive.
- When browsing the web, be careful to avoid unfamiliar links and instead enter URLs manually. If a link doesn't include "https" or the lock symbol in the search bar, then it's simply not secure. This is a red flag for a potentially fraudulent site.
- The physical security of your phone is also important. If you're in a crowded public space, keep your phone in a safe spot like your purse, pocket, or attached to you or a bag via a safety clip or lock. While it may not be the most convenient, this solution can prevent a thief from grabbing your phone out of your hands before you realize what's happening. It's always smart to be aware of your surroundings.
- If your phone is lost or stolen, there are several preventative security measures you can put in place beforehand so the damage is, well… less damaging. Always enable an access password to unlock your phone. Whether this is a code, fingerprint, or face recognition, it can stop or slow the rate at which the thief can access and transfer your information. If your phone is officially gone, there are ways to remotely wipe your phone data so the damage is even less severe.
- Malware can also apply to smart phones, so be cautious of what files you download and what links you click on. This is especially true for applications that monitor your sensitive information such as travel plans or online passes.
- It's tempting to delay software updates, but try to install them as soon as they become available. The software versions are created for a reason, and they usually include security upgrades.
- If you sell or trade-in your phone, be sure to either wipe the data clean or pay for an outside vendor to erase it.

How You Can Protect Yourself

- Destroy private records and statements when you are done with them. Tear, cut, shred, or burn paper items.
- Never give out checking account, credit card, or social security numbers to any unknown caller or unsolicited contact.
- Expect your monthly financial statements and bills. If you do not get them when expected, contact the sender and ensure that they were sent and that the address is still correct.
- Review your bank and financial statements. Verify all transactions were legitimate.
- Make a photocopy of information in your wallet, including both sides of your driver's license and any credit, ATM, debit, or merchant cards you carry with you. Keep the copy in a secure location other than your wallet. If your wallet is lost or stolen, you will know which cards you need to cancel and what personal information has been compromised.
- Review your credit report annually. By law you can receive a free credit report each year. Look through the report carefully to see if there is any suspicious activity. If so, contact your credit card company immediately. This report can be requested online at www.annualcreditreport.com, via telephone at 877-322-8228, and via mail at:

  Annual Credit Report Request Service
  P.O. Box 105281 Atlanta, GA 30348.5281
  (There is a specific form for the request available on the website).

What to do if You Become a Victim of Identity Theft

If you believe that you have been the victim of identity theft, the following actions will help minimize your exposure.

- Iroquois Farmers State Bank customers should contact us immediately at 815-698-2346. We will secure your Iroquois Farmers State Bank accounts and help with an identity theft toolkit for other financial relationships.
- File a police report with local authorities.
- Contact the fraud departments of the 3 credit bureaus below. Place a fraud alert and request a copy of your credit report.
- File a complaint with the Federal Trade Commission, by clicking on this link, Report Fraud or via telephone at 877-438-4338.

  Trans Union: 800-680-7289
  Experian: 800-397-3742
  Equifax: 800-525-6285

Additional Resources

For more information on identify theft and other account fraud, you can visit the following websites.

National Fraud Information

Federal Deposit Insurance Corporation

Federal Trade Commission on Identity Theft

Anti-Phishing Working Group

Microsoft

Lost or Stolen Debit Cards?

(800) 472-3272