Consumer Awareness Guide

While we cannot guarantee that your ID will never be stolen we will NEVER request personal information by email or text messaging including account numbers, passwords, personal identification information or any other confidential customer information.

Fraudulent emails may be designed to appear as though they are originated by Jarrettsville Federal. Do not respond to any email communications which request any type of personal or confidential information and do not go to any links listed on that email. These communications are not originated by Jarrettsville Federal!

Never give out any information that the Bank already has to a caller, texter, or email sender. If you contact us we may verify the last 4 digits of your SSN, or the date of your last deposit to confirm your identity but we will never contact you and ask for your debit/credit card number or your full SSN. If we need to contact you, it will always be done in a manner that protects your personal, confidential information and we will clearly identify ourselves.

One of Jarrettsville Federal's top priorities is to safeguard YOUR confidential information and we work diligently to do so.

We always work with the local regulatory and law enforcement departments to be certain any type of illegal activity is stopped as soon as possible. We have multi-layer security to protect your confidential information and will continue to be vigilant in protecting it.

Immediately report any suspicious emails or websites to Jarrettsville Federal by forwarding the message to help@jarrettsvillefederal.com. If you suspect identity theft or have any questions regarding this notice, please contact us at (410) 692-5151.

What is Identity Theft?

Identity theft involves the unlawful acquisition and use of someone's identifying information, such as:

- Name
- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Driver's License
- Bank or Credit Card Account Number

Thieves then use the information to repeatedly commit fraud in an attempt to duplicate your identity which may include opening new accounts, purchasing automobiles, applying for loans, credit cards, and social security benefits, renting apartments and establishing services with utility and telephone companies. It can have a negative effect on your credit and create a serious financial hassle for you.

How do I protect myself?

- Report lost or stolen checks or credit cards immediately
- Never give out any personal information including birth date, SSN or Passwords
- Shred all documents containing personal information, like bank statements, unused checks, deposit slips, credit card statements, pay stubs, medical billings, and invoices
- Don't give any of your personal information to any web sites that do not use encryption or other secure methods to protect it

Credit Reports

You have the right to request one free copy of your credit report from each of the credit reporting agencies once per year. Contact all three of the major credit reporting agencies below to request your free report. Consider rotating the requests by ordering one report every fourth months instead of contacting all three credit reporting agencies at the same time.

- Equifax: 1-800-685-1111
- Experian: 1-888-397-3742
- Trans Union: 1-800-916-8800

Debit Card Protection

Debit card usage has increased dramatically in recent years and fraudulent use of debit cards has also increased.

We at Jarrettsville Federal have some suggestions for you for the care and usage of debit cards.

- NEVER give your debit card information when requested by phone, email, or texting. We at neither Jarrettsville Federal nor any other bank we know of will ever request information from you in this manner. Please contact us if you receive any such request.
- It is a good idea to pay by credit card if your card leaves your sight. An example might be when a waiter takes your card from your table in a restaurant or when ordering online. Debit cards are easier to process illegally vs. credit cards.

Social Engineering

In terms of information security, social engineering is a broad term used to describe tools and techniques that criminals use to learn more information about an individual or a business, and the technology they use. It relies heavily on human interaction and often involves tricking people to breaking normal security procedures, thus providing the criminal with important information that can be used to commit fraud.
Social engineering can take on many different forms. Some examples of social engineering include, but are not limited to:

- Emails
    - With viruses/malware/spyware attached or that includes a link to viruses/malware/spyware.
    - That notifies the recipient of a suspended debit/credit card that requests a card number, PIN, or other information.

- Claiming the recipient has won a lottery or is listed as an heir in a will.

- Phone Calls
  - Pretending to be a representative of their financial institution and requesting personal and confidential information, such as Social Security number, account number, personal identification number (PIN), etc.
  - Pretending to be a lottery presentative who notifies you that you have won money in a lottery.
  - Pretending to be your grandchild who is in a foreign country and needs money wired for a problem they have encountered. The caller typically asks the grandparent not to contact "mom or dad" because they will be mad about the situation. The caller often sounds like the grandchild and uses sympathy as means of convincing the grandparent to wire money.
  - For any reason, asks you to send a wire transfer from a non-bank. Bank employees are trained to recognize fraud and criminals know a wire is more likely to be completed when a bank is not involved.
  - Automated phone call (also known as a robocall) notification of some sort of problem with your bank account or debit/credit card, and asks you to enter your PIN or card number.

- Text Messages
  - Claiming your debit/credit card is suspended or that fraud has been detected, and asks you to reply with your card number, PIN, or other confidential information.

- Dumpster Diving
  - The criminal goes through your garbage when placed outside for collection, looking for confidential information about you or your family.

- Media Drop
  - Criminal leaves flash drives or CDs in a public area hoping someone picks up the item and uses their computer to see what is on the media. Simply using the media loads a virus, malware, or spyware on your PC.

Security Tips

Passwords

- **Create a unique password for all the different systems/websites you use.** Otherwise, one breach leaves all your accounts vulnerable.
- **Never share your password over the phone, in texts, by email, or in person.** If you are asked for your password it's probably a scam.
- **Use unpredictable passwords** with a combination of lowercase letters, capital letters, numbers, and special characters.
- **The longer the password, the tougher it is to crack.** Use a password with at least 8

characters. Every additional character exponentially strengthens a password. Passphrases are most effective. A passphrase is a short sentence and generally easier to remember.

- **Avoid using obvious passwords** such as:
  - Names (your name, family member names, business name, user name, etc.)
  - Dates (birthdays, anniversaries, etc.)
  - Dictionary words
- **Choose a password you can remember without writing it down.** If you do choose to write it down, store it in a secure location.

Email Security

- **Scrutinize emails carefully** before clicking on links or opening attachments in emails, even if they appear to be from someone you know. Many times, these emails will appear to be authentic and claim to be from your bank, credit card company, or another trusted source. They may ask you to verify information about your account. DO NOT respond to these emails, DO NOT click on links in these emails, and DO NOT open attachments in these emails.
- **Do not call phone numbers** provided in a suspicious email. It is likely a "fake" phone number monitored by a criminal. Always contact your bank, credit card company, or other trusted business using a phone number provided on their published website or other trusted source.
- **Email is not secure,** and you should never send an email to your bank that contains confidential information. At Jarrettsville Federal, you can send us confidential information electronically as follows:
  - Log in to Internet Banking and click the envelope symbol in the upper left corner of the screen.

Online Security

- **Never click on suspicious links** in emails, tweets, posts, or online advertising**.** Links can take you to a different website than their labels indicate. Typing an address in your browser instead of clicking a link in an email is a safer alternative.
- **Only submit sensitive information to websites using encryption** to ensure your information is protected as it travels across the Internet. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://". Some browsers also display a closed padlock.
- **Do not trust sites with certificate warnings or errors.** These messages could be caused by your connection being intercepted or the web server misrepresenting its identity.
- **Avoid using public computers or public wireless access points** for online banking and other activities involving sensitive information when possible.
- **Always "sign out" or "log off"** of password protected websites when finished to prevent unauthorized access. Simply closing the browser window may not actually end your session.
- **Be cautious of unsolicited phone calls, emails, or texts** directing you to a website or requesting information.

- **If you download anything from the Internet** (such as music, pictures, videos, software, etc.), make sure you download only from a trusted source. Downloaded files can contain harmful threats to your PC, such as viruses, malware, spyware, etc.
- **Make online purchases only from trusted web sites.** Research unknown companies before making an initial purchase. The Better Business Bureau is a good resource.

Mobile Device Security

- **Configure your device to require a passcode to gain access** if this feature is supported in your device.
- **Avoid storing sensitive information.** Mobile devices have a high likelihood of being lost or stolen so you should avoid using them to store sensitive information (e.g. passwords, account numbers, etc.). If sensitive data is stored, enable encryption to secure it.
- **Keep your mobile device's software up-to-date.** These devices are small computers running software that needs to be updated just as you would update your PC. Use the automatic update option if one is available.
- **Review the privacy policy and data access of any applications (apps)** before installing them. Only download apps from trusted app stores (Apple, Google Play).
- **Disable features not actively in use such as Bluetooth, Wi-Fi, and infrared.** Set Bluetooth- enabled devices to non-discoverable when Bluetooth is enabled.
- **Delete all information stored on a device before the device changes ownership.** Use a "hard factory reset" to permanently erase all content and settings stored on the device.
- **"Sign out" or "Log off" when finished with an app** rather than just closing it.
- **Utilize antivirus software** where applicable (i.e. Android, Windows, etc.).
- **Do not jailbreak** or otherwise circumvent security controls.

General PC Security

- **Maintain active and up-to-date antivirus protection** provided by a reputable vendor. Schedule regular scans of your computer in addition to real-time scanning.
- **Update your software frequently** to ensure you have the latest security patches**.** This includes your computer's operating system and other installed software (e.g. web browsers, Adobe Flash Player, Adobe Reader, Java, Microsoft Office, etc.).
- **Automate software updates,** when the software supports it, to ensure it's not overlooked.
- **If you suspect your computer is infected with malware,** discontinue using it for banking, shopping, or other activities involving sensitive information. Use security software and/or professional help to find and remove malware.
- **Use firewalls** on your local network to add another layer of protection for all the devices that connect through the firewall (e.g. PCs, smart phones, and tablets).
- **Require a password to gain access.** Log off or lock your computer when not in use.
- **Use a cable lock to physically secure laptops** when the device is stored in an untrusted location.

- **Keep your computer's operating system up-to-date** with the latest security patches provided by the operating system vendor. Turn on automatic updates and keep your firewall on at all times.
- **Take immediate action if you see signs of spyware** on your PC. This includes pop-up ads, icons on your desktop, error messages, sluggish/slow PC performance.

Resources

The following links are provided solely as a convenience to our Online Banking customers. We neither endorses nor guarantees in any way the organizations, services, or advice associated with these links. Jarrettsville Federal is not responsible for the accuracy of the content found on these sites.

FDIC – Electronic Funds Transfers (Regulation E)

https://www.fdic.gov/regulations/laws/rules/6000-1350.html

Protecting Personal Information: A Guide for Business

https://www.ftc.gov/news-events/audio-video/video/protecting-personal-information-guide-business-promotional-video

Consumer Action: Complaints

http://www.usa.gov/topics/consumer.shtml

FDIC Consumer Protection

http://www.fdic.gov/consumers/

FDIC Consumer Alerts:

http://www.fdic.gov/consumers/consumer/alerts/index.html

ID Theft

http://www.ftc.gov/bcp/edu/microsites/idtheft/

NACHA Fraud Resources

https://www.nacha.org/for-consumers

US Department of Homeland Security

http://www.us-cert.gov/home-and-business/

Federal Communication Commission - Business Cyber-planner:

http://www.fcc.gov/cyberplanner

On Guard Online:

http://www.OnGuardOnline.gov

Better Business Bureau

http://www.bbb.org/council/data-security-made-simpler/

United States Computer Emergency Readiness Team:
https://www.us-cert.gov/