

Avoid Phishing Scams

Phishing is an email scam involving fraudsters who pretend to be a legitimate business such as a financial institution, credit card company, online service provider, or retailer. Hiding behind the anonymity of the internet, they send out “official looking” emails or set up bogus websites to trick you into divulging your account numbers, passwords, social security numbers, and other sensitive data. **Independent Bank will never send email messages asking you to verify or provide personal information such as your social security number, account number, debit card number, or passwords.**

We suggest forwarding a phishing email or spoofed website to the following groups:

- reportphishing@antiphishing.org
- spam@uce.gov
- spoof@ebay.com
- File complaint with the Internet Crime Complaint Center of the FBI at www.ic3.gov.

Protect Yourself from Online Fraud

- Treat unsolicited email requests for financial information or other personal data with suspicion. Do not reply to unsolicited email or respond by clicking on a link within an unsolicited email message.
- Contact the actual business that supposedly sent the email to verify if it is genuine. Visit a website or call a phone number that you know to be legitimate.
- Prior to entering account information on any website, be sure to look for the “locked padlock” to make sure the site is secure.

Other Tips to Keep Personal Information Safe

- Review your credit reports frequently. For a free copy of your credit report go to www.annualcreditreport.com or call toll free 1-877-322-8228.
- Do not place outgoing mail in your residential mailbox.
- Implement a clean desk policy at home.
- Never give personal information over the phone or internet.
- Beware of mail, email, and telephone solicitations.
- Invest in a shredder that makes tiny pieces of confetti.
- Never leave receipts at ATMs (Automated Teller Machine), bank workstations, trash receptacles, or unattended gas pumps.
- Sign all credit cards upon receipt.
- Use a blue or black gel ink pen when signing checks and credit cards.
- Review your credit card statement as soon as it arrives.
- Check all your personal and business accounts frequently.
- Always shield your pin numbers when using an ATM.
- Only use essential information on your checks – no birth dates or social security numbers.
- Lock your bank check stock in a safe place.
- If an investment proposition seems “too good to be true” it probably is.