THE LYONS STATE BANK

Tips on how to keep your information safe

The officers and staff at The Lyons State Bank care about our customers and the money entrusted to us. Also, we are committed to protecting our customers' information by complying with laws and regulations and adhering to solid internal procedures, such as strict confidentiality. Our employees are trained to perform their regular duties and, we're also trained to be watchful of unusual account activity that could result in a loss to an unsuspecting customer. We're not afraid to ask questions and that's what we strongly recommend to our customers who receive suspicious, unexpected phone calls.

No one wants to be scammed or taken advantage of and we certainly don't want to lose our money or our personal information. But yet, thousands of phone calls are placed every day by deceptive individuals who prey on innocent victims. Persons calling your house phone or cell phone can be very convincing and seem sincere. They can even lead you to believe some of your personal details are already known to them. The caller ID indicates a town or city familiar to you.

How can you prevent becoming a victim?

• Develop a healthy sense of skepticism and ask questions.

• Keep a pen and paper close by for notes.

• Don't commit to anything and don't reveal your social security number, bank info or credit card number.

• Once you're off the phone and have a computer, Google the company name and look for scams.

• Still not sure? Tell someone at The Lyons State Bank what has happened. We'll do our best to answer all your questions and protect your funds.

• If all else fails and you still get phone calls, don't answer. Let your message machine or voice mail do the work for you. You can return legitimate phone calls at your convenience.

• Consider listing your number on the Do Not Call list – which is free. You have to call from the number to be listed: 1-888-382-1222.

• Other good information about stopping nuisance phone calls is available at the Federal Trade Commission website: https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry.

Also from the FTC website is the following information about common scams:

IMPOSTER Scams

You get a call or an email. It might say you've won a prize. It might seem to come from a government official. Maybe it seems to be from someone you know – your grandchild, a relative or a friend. Or maybe it's from someone you feel like you know, but you haven't met in person – say, a person you met online who you've been writing to.

Whatever the story, the request is the same: wire money to pay taxes or fees, or to help someone you care about. But is the person who you think it is? Is there an emergency or a prize?

Judging by the complaints to the Federal Trade Commission (FTC), the answer is no. The person calling you is pretending to be someone else.

Here's what you can do: Stop and check it out – before you wire money to anyone. Call the person, the government agency, or someone else you trust. Get the real story. Then decide what to do. No government agency will ever ask you to wire money.

IRS Scams

You get a call from someone who says she's from the IRS. She says that you owe back taxes. She threatens to sue you, arrest or deport you, or revoke your license if you don't pay right away. She tells you to put money on a prepaid debit card and give her the card numbers. The caller may know some of your Social Security number. And your caller ID might show a Washington, DC area code. But is it really the IRS calling?

No. The real IRS won't ask you to pay with prepaid debit cards or wire transfers. They also won't ask for a credit card over the phone. And when the IRS first contacts you about unpaid taxes, they do it by mail, not by phone. And caller IDs can be fake (to conceal their actual location and hide from law enforcement).

Here's what you can do: Don't wire money or pay with a prepaid debit card. Once you send it, the money is gone. If you have tax questions, go to irs.gov or call the IRS at 800-829-1040.

ONLINE DATING Scams

You meet someone special on a dating website. Soon he wants to move off the dating site and communicate via email or phone calls. He tells you he loves you, but he lives far away — maybe for business, or because he's in the military. Then he asks for money. He might say it's for a plane ticket to visit you. Or emergency surgery. Or something else urgent.

Scammers, both male and female, make fake dating profiles, sometimes using photos of other people — even stolen pictures of real military personnel. They build relationships — some even fake wedding plans — before they disappear with your money.

Here's what you can do: Don't send money. Never wire money, put money on a prepaid debit card, or send cash to an online love interest. You won't get it back.

TECH SUPPORT Scams

You get a call from someone who says he's a computer technician. He might say he's from a well-known company like Microsoft, or maybe your internet service provider. He tells you there are viruses or other malware on your computer. He says you'll have to give him remote access to your computer or buy new software to fix it.

But is the caller who he says he is? Judging by the complaints to the Federal Trade Commission, no. These scammers might want to sell you useless services, steal your credit card number, or get access to your computer to install malware, which could then let them see everything on your computer.

Here's what you can do: Hang up. Never give control of your computer or your credit card information to someone who calls you out of the blue.

YOU'VE WON Scams

You get a card, a call, or an email telling you that you won! Maybe it's a trip or a prize, a lottery or a sweepstakes. The person calling is so excited and can't wait for you to get your winnings.

But here's what happens next: they tell you there's a fee, some taxes, or customs duties to pay. And then they ask for your credit card number or bank account information, or they ask you to wire money. Either way, you lose money instead of winning it. You don't ever get that big prize. Instead, you get more requests for money, and more promises that you won big.

Here's what you can do: Keep your money – and your information – to yourself. Never share your financial information with someone who contacts you and claims to need it. And never wire money to anyone who asks you to.

Want to know more? Sign up for scam alerts at ftc.gov/subscribe.

If you spot a scam, please report it to the Federal Trade Commission.

• Call the FTC at 1-877-FTC-HELP (1-877-382-4357) or TTY 1-866-653-4261

• Go online: ftc.gov/complaint

Your complaint can help protect other people. By filing a complaint, you can help the FTC's investigators identify the imposters and stop them before they can get someone's hard-earned money. It really makes a difference.

Finally, report the attempted scam to The Lyons State Bank. Scammers may be targeting others in our community. We'll assist you in taking the next step to protect your funds.

Mark Your Calendar now.
Annual Shred Day is June 9!
Securely destroy your old statements and documents. FREE!