



INFORMATION ABOUT SCAMS

FOR RESIDENTS

A Word From The Chief...

Each week, too many of our residents become victims of financial fraud – whether through a scam, a data breach or identity theft.

Scams, (also called “Crimes of Persuasion” because you have been persuaded to part with money or information) can happen on your phone, on your computer or even at your door.

Identity theft can involve the use of your social security number, date of birth, debit or credit card, bank account, license – even your medical information.

And a data breach can happen to any of us at any time without our knowledge.

We are providing this information for residents to help you protect your information and to minimize financial loss.

Patricia Arnaudin
Chief of Police
(207) 646-9362

Scammers Can Be Anywhere

Scams are called “crimes of persuasion” because the scammer tries to persuade the victim to give them information or send money. They do this by pretending to be a legitimate business or organization.

They often ask you to send them money using services like Western Union or MoneyGram. They may also ask you to purchase a pre-paid card or gift card to make your payment to them. Cards that are frequently suggested by scammers are iTunes and Green Dot cards. If you are asked to use one of these methods to send money, it may be a scam.

In addition to asking you to send money, scammers can also try to trick the victim into giving information over the phone or via email. Be careful not to provide your credit card, debit card or bank account information – or give your social security number or date of birth – to strangers over the phone or online.

Before you give information or rush to send money to someone you don’t know, stop and consider that this may be a scam. Unfortunately, once you have sent money to the scammer, it can be impossible to obtain a refund and your money could be gone forever. Because Medicare account numbers are your social security number, be careful about giving that number to anyone over the phone or via email.

In September, 2017, Equifax announced a massive data breach that affected 145.5 million records.

Scammers are taking advantage of this data breach using phones and emails to try to convince victims to provide them with information. DO NOT provide information over the phone or via emails and DO NOT open attachments or click on links in emails.

Because of this breach, we advise Maine residents to contact the three credit bureaus (Equifax, Experian and TransUnion) to place a security freeze on their credit reports. In Maine, there is no charge to place the security freeze which is protected by state law, unlike the “security locks” being offered.

Here are the phone numbers to call to place a security freeze on your or your child’s credit file:

Transunion – 1-888-909-8872

Experian – 1-888-397-3742

Equifax – 1-800-685-1111 option 3

To help you recognize a possible scam, here is more information about this activity and some real life examples.

On your phone...

Scammers rely on catching you off guard and they create a sense of urgency by telling you that something terrible will happen unless you act immediately. Or they may promise you that you have a limited time to take advantage of their offer or it will be gone. If you receive a call like this, hang up the phone immediately. Here are some examples of phone scams taken from real situations:

#1 "Help, grandma/grandpa, I'm in trouble!"

The victim received a telephone call from a scammer saying that the victim's grandchild had been arrested. The call may come from someone claiming to be the grandchild.

#2 "IRS calling. You owe money for taxes."

The caller claims to be an IRS agent threatening you with fines or arrest for not paying them enough in taxes. If you think you've been contacted by an IRS scammer you should call the Treasury Inspector General for Tax Administration at 1-800-366-4484.

#3 "Limited time offer for a government grant."

Scammers say they are government officials with an offer to get a grant for a "processing fee."

#4 "A debt must be paid immediately."

Scammers say that you have an old debt that must be paid immediately or you will be arrested and go to jail.

#5 "This is John from Microsoft and your computer needs to be fixed."

The scammer calls you pretending to be from a legitimate computer company and saying that they have discovered a problem with your computer that needs to be fixed immediately.

#6 "We are counting on you to contribute to our charity."

The scammer pretends to be from a charity and asks you to make a contribution to them by giving your credit card or debit card information or by sending money. These calls can occur immediately after a publicized event like a weather (or other) disaster. Ask the caller to send you the information to you in the mail so you can review it. You can contact the BBB at 703-276-0100 or Charity Navigator to ask about the charity.

#7 “Congratulations! You’ve won!”

The scammer calls to tell you that you won a free vacation, prize or lottery, but in order to collect the prize, you must first pay them some sort of fee or tax. And you should know that Federal law prohibits the cross-border sale or purchase of lottery tickets by phone or mail, so foreign lotteries are illegal in the U.S.

#8 “Your service will be disconnected unless you pay immediately.”

Scammers call a victim and tell them that their phone, electric or other service will be disconnected unless the victim pays them immediately by giving them their credit or debit card information.

#9 Don’t Say “YES!”

Scammers are using recordings of a victim’s own voice to try to convince them to send money.

When the victim answers the phone, the scammer asks “Can you hear me?” or some other question. When the victim answers “yes” the response is recorded and the scammer later uses that recording to try to convince the victim that they have agreed to pay the scammer money.

It is important to know that just because you hear a recording of your voice saying “yes” it does not mean that you owe anyone money. The debt would only be valid if both parties know what is being offered and agree to the payment for services or goods.

#10 Caller ID Looks Like a Local Number

Technology has given scammers the ability to “spoof” other telephone numbers. When a number is “spoofed,” the scammers display a legitimate phone number on your caller ID – sometimes showing the local police department or court - so you think the person calling you can be trusted. Be cautious and don’t believe what your caller ID displays – the incoming call could be coming from a scammer located anywhere in the world.

On your computer...

Every year, billions of dollars are spent using the internet. Make sure that your information, your accounts and your devices are safe while you shop. And since at least half of all purchases will be made using a cell phone or a tablet, here is some advice concerning these, too.

- Make sure that your devices (computers, cells and tablets) have the recommended security software and settings and that you have installed all updates.

- Use a credit card, not a debit card. The federal laws that govern credit card purchases offer you more protection than laws that govern debit card purchases.
- If you are shopping online, DON'T use a public Wi-Fi network. Use only Wi-Fi that is private and secure.
- Be careful of ads that appear on social media sites. Check out the business before clicking on a link or attachment.
- Use caution if you see pop up ads that offer drastic Black Friday discounts. These may be phishing attempts.
- Enable 2-factor authentication for your apps.
- If you are using your cell or tablet, use the business's app instead of your browser.
- Make sure that the website you are using for an online purchase includes "https" and shows this:



A word about phishing...

What is "phishing"? Phishing (pronounced just like "fishing") is a type of scam that is conducted via email or text. The thief will send a message that misleads the victim into believing it is real. The thief will then request information from the victim that can be used to steal their money. The thief may also entice the victim to open an email attachment that can obtain information stored on the victim's computer.

A word about malware and ransomware:

Malware is malicious software that can enter your computer system through links that are contained in phishing emails and on certain websites. Malware can be designed to do any one of several different things.

Some malware may use the email addresses on your computer and while pretending to be you, send false messages to your contacts asking for money.

Some malware may scan your system for your personal information, looking for your online banking or payment transactions and use these to access your accounts.

And then there is malware called “ransomware.” Its job is to enter your computer and encrypt what’s on it, so it becomes inaccessible to you. It then demands a payment from you to unlock your computer files.

Do not open links in email messages or on websites unless you are certain of their origin.

To help you recognize phishing messages, here is more information about this activity and some real life examples.

#1 “Reactivate your account.”

The victim is asked to provide information online to reactivate their debit, credit card or other financial account.

#2 “I want to buy your Craigslist item.”

The victim is contacted in response to an ad on Craigslist and the scammer sends a payment that is more than the amount advertised, asking the seller (who is the victim) to send the additional amount to a third party.

#3 “You can work from home.”

Scammer contacts victim by email or phone and “hires” them. The work involves cashing checks and/or forwarding letters or packages to another address. In the case of the “Secret Shopper” scam, the victim will be told to shop with a check that appears to be good but is not.

#4 “Help me and I’ll share the money with you.”

Known as the Nigerian scam, the victim is contacted by someone who needs help getting a vast sum of money out of a bank or country. They are offered some of the money if they assist the scammer.

#5 “She (or he) loves you.”

The scammer begins an online relationship with the victim, eventually asking for the victim to provide money for some bogus reason.

#6 “Doing God’s work.”

The scammer takes advantage of the victim’s religious beliefs, asking for money for a religious project or program.

#7 “Here is the information about your invoice.”

The scammer tries to lure the victim into opening an attachment by claiming that it is an invoice that must be paid or a reservation that has been made.

#8 “Your delivery is scheduled for tomorrow.”

The scammer tries to lure the victim into opening an attachment by claiming that it concerns delivery of an item. DO NOT OPEN any links contained in an email about a package delivery. On its website, UPS specifically says: “UPS does not request payments, personal information, financial information, account numbers, IDs, passwords, or copies of invoices in an unsolicited manner through email, mail, phone, or fax or specifically in exchange for the transportation of goods or services.”

At your door...

Scammers aren’t just operating on the phone or over the internet. Every year local police departments receive calls from residents who have been scammed by people who ring the doorbell, claiming to be someone they are not. Be particularly wary if you have recently had a storm because scammers follow storms offering to clean up a victim’s property for a fee.

In Maine, anyone who is selling a service door-to-door is subject to a state law that requires them to register with the local police and wait three days before beginning the work or receiving payment.

Don’t open your door to anyone you don’t know – no matter what they say.

Here is more information about this activity and some real life examples:

#1 “We have asphalt left over.”

The business offers to use up their left over asphalt from another job by fixing your driveway for a discounted price.

#2 “We’re offering discounted magazine subscriptions.”

Scammers particularly target the elderly with sales of magazine subscriptions and the victim is often enrolled in a five- or ten-year subscription plan.

#3 “Where’s the beef?”

Some scammers arrive at a victim’s door selling what they claim is USDA certified beef for a discounted price. The victims find that they have purchased beef that is inedible.

#4 “Couldn’t your floor be cleaner?”

Scammers sell cleaning products at a highly inflated price and lock the victim into a long financing period.

#5 “There have been robberies in the area.”

The scammers create fear in their victims and use this to sell them worthless home security systems. They also try to gain access to the residence by offering a free security check.

If you gave any of the following information to a scammer...

- Debit or credit card
- Bank account number
- Social security Number
- Date of birth
- Driver’s license number
- State identification/Medicare card number
- Account passwords, pins or other access codes

Scammers may use your information to commit identity theft. Please ask our department for a copy of the data breach and identity theft booklet which gives you information about what to do if your information was released.

If you sent money to a scammer, immediately report the fraud:

- Western Union..... (800) 448-1492**
- MoneyGram..... (800) 926-9400**
- Green Dot Card..... (866) 795-7597**
- iTunes Card (Apple)..... (800) 275-2273**

HERE ARE OTHER AGENCIES THAT MAY BE HELPFUL:

Federal Trade Commission:

Customer Service 1-877-382-4357 press 0 and 3

To sign up for email scam alerts from the FTC:

<https://www.consumer.ftc.gov/scam-alerts>

To list your phone on the Do Not Call Registry: 1-888-382-1222

Or: <https://www.consumer.ftc.gov/scam-alerts>

(Important- Call from the phone you want to list)

Internal Revenue Service Fraud Line 1-800-366-4484

U.S. Senate Special Committee on Aging:

Fraud Hotline 1-855-303-9470

Maine Attorney General Consumer Protection 1-800-436-2131

Maine Bureau Of Financial Institutions 1-800-965-5235

Office of Consumer Credit Regulations 1-800-332-8529

Charitable Contributions:

Dept. Of Professional & Financial Regulations) 1-207-624-8603

Charity Navigator 1-201-818-1288

www.charitynavigator.org

Debt Collection:

Consumer Credit Regulations 1-800-332-8529

Internet Fraud Complaint Center:

<http://www1.ifccfbi.gov/index.asp>

U.S. Postal Inspector (Maine) 1-207-871-8587

Social Security Administration (SSA) 1-800-269-0271

Veterans Services 1-800-827-1000