‘Scares Me To Death’

Fraud Prevention Expert Speaks To The Vermillion Rotary

Vermillion Plain Talk
Serving our readers since 1884.

By Sarah Wetzel for the Plain Talk May 10, 2024

https://www.plaintalk.net/local_news/article_918a8ec2-0e3e-11ef-b4fa-7f26c2f3d554.html

Kevin Watt, fraud prevention expert at First Dakota Bank, spoke at a recent Vermillion Rotary Club meeting to educate his audience about the ever-growing danger of fraud and identity theft.

Though not a fun topic, Watt stressed the importance of it.

“It is an ever-growing epidemic so we like to get out as much as we can to talk about what we’re seeing these days and ways to try to protect yourself,” he said.

According to Watt, the average loss for fraud victims is $500 with the top 15% losing $10,000 or more.

“Fraud and identity theft do not discriminate,” he said. “Anybody’s vulnerable, 16 to 90, doesn’t matter what age group you’re in. They’re making attempts on you almost on a daily basis.”

Watt said it’s very important to be proactive and think twice if you have any questions, suspicions or issues.

Kevin Watt, fraud prevention expert at First Dakota Bank, addresses a recent meeting of the Vermillion Rotary Club and shares steps that can be taken to avoid fraud and identify theft. “It is an ever-growing epidemic so we like to get out as much as we can to talk about what we’re seeing these days and ways to try to protect yourself,” he said. Courtesy of Vermillion Rotary Club

“Take action if something happens,” he said. “If it doesn’t look right, doesn’t smell right, follow your gut.”

Watt has seen an evolution in scams from when he started in the area about 12 years ago.

“The scams are pretty much the same but their approach and the technology they use is so much better today it’s much harder to fight,” he said. “It scares me to death, keeps me awake at night sometimes just because we don’t know what’s coming at us.”

A lot of the fraudulent companies are out of the country, making it difficult to get victims’ money back once it’s been taken.

One of the most important things to do if you’ve fallen for fraud, Watt said, is letting your financial institution know about it by calling the number on the back of your card and being honest about the situation.

“I always have people beating themselves up; they feel so stupid,” he said. “I say don’t beat yourself up. You’re not the first, you won’t be the last. Some of the smartest people I know have fallen for some of the most common scams.”

Watt reviewed some scam methods and what they might look like.

Imposter scams generally come in the form of a text or email claiming to be some form of government entity, insurance and benefits or utility company or even a business such as Amazon, PayPal, Venmo or Zelle.

The letter could say if you don’t pay a certain amount by a certain time your power will be cut off or you are being charged for something you did not purchase. Calling the number on the letter will direct you not to the company but to a fraudster.

“We were targeted by a group of people sending out texts saying hey you’ve got this charge for $982 and some odd cents, if that was not you click this link,” he said. “The link infected their phones immediately.”

Email compromise occurs when sensitive information on either side of an email exchange is intercepted by fraudsters. According to Watt,

businesses who use a lot of email should be wary of this.

"If one of the two sides of an email has been compromised you will start seeing a shift in the language and the people who compromised you are going to try to get you to send them money instead of to your vendor or whoever it is," he said. "Always confirm that whatever you're doing with your customer or your vendor is what you wanted to do."

Grandparent scams are when someone gets a message supposedly from a relative in trouble and in need of funds.

"Grandchild calls and says they're in jail down in Mexico or somewhere, they're in some sort of trouble, those are still pretty common," Watt said. "I will tell you with Artificial Intelligence coming online, that's going to get worse. If they somehow talk to your daughter, granddaughter, son, grandson and get a few snippets of their voice, they can put together a script that is perfectly in their tone range so AI is going to make our job and your job that much more difficult."

Other types of scams include tech support and customer service scams, romance and relationship scams, and grant and lottery scams.

Watt pointed out several common fraud techniques and ways to avoid falling for them.

One thing to do is to avoid mailing checks through an unsecured outgoing mailbox.

If thieves find a piece of mail with a check in it, not only do they suddenly have personal information such as an address and bank account number, but they also can lift the signature to be used on a counterfeit check or lift everything off except the signature and create a new check for themselves.

Watt also said it's important to keep an eye on your account even if you do have a secure way of mailing out checks in case the check gets stolen on the other end.

He said he is seeing a lot of person-to-person and bank-to-bank fraud, getting the victims to send money through things like PayPal.

"Wire fraud -- when we get wire requests we will do a call back to the sender of the wire. If you tell us those instructions are correct, we're going to send the wire," Watt said. "If you're going to do business that way, do your call back to the person who's going to receive the wire to make sure that you have the proper instructions as well.

"Cryptocurrency is getting bigger these days," he said. "If someone is asking you to put money in a crypto machine you're being scammed. No government entity is going to try to protect your money by having you put cash in a crypto machine. Crypto's a fine thing if you know what you're doing but most people don't."

Many scammers use stolen identities and information to open accounts for things like credit cards, mobile carriers, service or utilities.

"They open them not to put money in and save it, but they open them to funnel stolen money in and move it on through the banking system to launder it," Watt said.

He said banks look for red flags when looking at applications in case of fraud. Such red flags include phone numbers and email addresses that don't match the customer.

Scammers will also attempt to file fraudulent tax returns.

"If you're ever notified that you're an ID theft victim, that's one of the first things you want to do as soon as you can," Watt said. "The sooner you can file taxes the better."

He said scammers often sell personal information they have collected.

"If your social security number gets stolen, it costs about a dollar to sell it on the dark web," Watt said. "The more they have on you the more money they can make."

Some fraudsters will create a synthetic ID over time using a mix of different victims' information, making it hard to track.

"It can take them five years to get a good synthetic ID built, then they go on a rampage of borrowing money that they'll never pay back and banks get hung on that," he said.

Scammers are constantly trying to steal personal information for Identity theft using texts, emails, phone calls, data breaches and hacking.

Watt warned against leaving personal items like purses and wallets in your car or throwing things with sensitive information away.

"You put anything personal in your trash and take it back to the alley, it's public," he said. "Anybody can get in there, there's no law against that."

In the event that one encounters a potentially fraudulent situation, Watt said the most important thing is to keep a level head.

"I like to say stop and think," he said. "Trust your gut and respond accordingly."

Responses could be calling your bank, credit card company or family member. Talking it out can help figure things out.

"If you get the text, contact your bank to see if there actually was a charge; don't respond to the message," Watt said.

He said some red flags everyone should look out for include incorrect information, vague references, urgent language, misspellings and grammar issues and visuals.

"Most American companies will not use the term USD behind the dollars and cents," Watt said. "Some do but most don't. It's a red flag, doesn't mean it's necessarily fraudulent. 'That you are finding our services enjoyable is our goal,' we don't write that way."

Phrases like "Suspicious behavior has been observed, call us within 24 hours" puts pressure on the victim to act too quickly.

Checking phone numbers and return email addresses can reveal red flags, Watt said.

"If it really came from Amazon, it's going to have an Amazon email associated with it," he said.

Since prevention is always best, Watt recommends education on the issue.

"Understand the current scams," he said. "I just tell people go out to Google and say common frauds and scams. You will come up with scads of articles about what's going on out there and you can keep yourself informed about any new developments that there are."

Watt said he asks a lot of questions when people call for help with fraudulent situations in order to educate himself on scammer techniques.

Using trusted websites, phone numbers and contact methods throughout the process is also vitally important, he said.

"One of the biggest problems people have and get scammed for is they look for a phone number by Googling a major company," Watt said. "You don't have to Google the company. You go to their website."

People can also review accounts and statements and consider products and services such as facial recognition for devices and transaction alerts.

For businesses that write a lot of checks, there are services such as Positive Pay.

"You're going to have to upload a file of every check you write, you're going to upload the payee, you're going to upload the amount and you're going to upload the check number," he said. "If any of those don't match when they clear, a report's going to kick out and you're going to have to look at it. It costs a little money, takes a little effort but it only takes one bad check that you don't catch."

To detect mail theft as soon as possible, Watt recommends USPS Informed Delivery.

"They will send you a snapshot of every piece of mail that's coming to your mailbox every day," he said. "So if you see a picture of something that you don't end up receiving you'll know it's probably stolen. It's a handy tool because you'll know what's coming."

With so much information on devices, Watt said we need to keep devices password protected, refrain from clicking on suspicious links or attachments and don't allow someone to "watch" your device.

Private information should also be protected by shredding personal documents and avoiding oversharing on social media.

"Don't put a lot of personal information and avoid games where they're trying to get you to say what's your favorite color, etc," Watt said. "They're getting hints on what might be your passwords.:

Watt also recommends monitoring your credit which you can do for free on annualcreditreport.com.

"I recommend you keep a fraud alert on there at all times," Watt said. "They stay on there for one year. They tell any lender who pulls your credit report for the purpose of issuing credit, I am an ID theft victim. Do not issue credit without calling me."

If you fall victim to a fraud, Watt said to contact local authorities, report to the appropriate government agency such as the Federal Trade Commission or the FBI Internet Crime Complaint Center and contact creditors and financial institutions.

"Don't be afraid to call us and say hey I made a mistake today, here's what happened, can you help me out," Watt said. "I know it's embarrassing to do that but it's the best way that we can figure out exactly what happened."