Bank of Botetourt

December 2021

Member FDIC

EQUAL HOUSING LENDER

You may have survived the scams of 2021, but are you ready for 2022?

Time to say goodbye to 2021 and the scams of yesteryear.

Hopefully, you weren't a victim this year. But from everything I've read this year, it's a pretty safe bet you were a target.

Going out on a short limb here, it's another safe bet you'll be targeted again.

Most of us have been in scammers' sights at some time. For instance, multiple sources shows that half of us have had our social media accounts compromised. Virtually all of us have also had personal information stolen in data breaches. The FBI reports it receives more than 800,000 internet crime reports every year, that adds up to an estimated $4 billion in losses.

As the online crime rate continues to rise, you need to be on your guard 24/7. It's only a matter of time. One thing you can count on — scammers mostly want just one thing, our money. They get it either by tricking you into giving it to them or by stealing or buying information about you to commit identity theft.

COVID hasn't helped things either. In the past year, the ongoing pandemic has sparked lots of tricks, such as stimulus check scams and phony COVID cure or protection claims.

Other areas that have seen a scam surge during 2021 include ransomware, government impostors, cybercurrency fraud, dishonest influencers, charity collectors, and phony tech support.

Continued on Page 2

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt
(540) 591-5000

So, what's expected to happen next year? Based on current trends, reported by Scambusters and what we see in the BBB Scamtracker here's where you can expect to see more scams than ever in 2022.

Ransomware

Which involves hacking or sneaking onto someone's computer and locking it until a ransom is paid -- is expected to be the fastest growing cybercrime in 2022, after climbing more than 20 percent this year. It's mostly aimed at big organizations, but individuals are targeted, too.

Malware and Hacking

Cons are finding new ways to get onto your PC by tricking you into downloading files that steal information or turn your device into a "zombie" botnet (robot network) for spamming.

Impostors

The crooks will say they're from the IRS, Social Security Administration, lottery promoters, utility companies, banks and card companies, or even a friend or relative in distress. They'll ask for payment using some untraceable methods such as money wiring services, Bitcoin payments, gift cards and, oddly cash.

Phishing

Scammers love phishing -- tricking you into giving away personal information via impostors, fake website pages, email, text, and illegal robocalls. Being on the do-not-call register, is smart but it won't protect you from the scammers because they simply ignore it.

Fake offers

More of us than ever are shopping, and doing investment and information searches, online. The incidence of fake offers will continue to rise.

Data Breaches

There's no reason to think the theft of customer data from big organizations will slow down in the coming year. The black-market cost for an individual's confidential information is falling, so crooks need to increase the amount they steal.

So how do you protect yourself? There are some simple things to do like always being skeptical and researching everything before you act. Here's a list of other tips:

- Use of multi-factor authentication (MFA).
- Don't be too trusting. Question.
- Only buy from or invest with companies you've thoroughly checked out.
- Don't be over-confident. Even security specialists get tricked every day. And millennials fall for scams more often than older folk.
- Never pay by the untraceable methods that I mentioned.
- Keep tabs on your financial accounts, your credit report and score, and know how to freeze your credit via your bank and the big three reporting agencies.
- Don't share everything about yourself and your family on social media.
- Back up your computer system regularly and your data every day.
- Don't answer robocalls. They're almost all illegal. Use your voicemail or a call blocker to protect you.

Happy New Year and stay safe in 2022!

Source:

Dennis Horton, Director of the Rockford Regional Office of the Better Business Bureau, Special to the Rockford Register Star, Published 1:00 PM CT December 23, 2021

If You Get These Texts, Delete Them Immediately

Friends and family aren't the only ones who text you. Scammers do too!

Like the old adage about finding true love goes, "There are plenty of fish in the sea!" In the digital world of cyber hacking, they're known as "phish," a scamming tactic used to trick people into revealing confidential information about their bank account, credit card, or other personal accounts. These phishing attempts first started out as phone calls and emails, but now cybercriminals can also reach you via SMS (text message) through a popular phishing scam dubbed "smishing."

A good general rule of thumb for a text from someone you don't know is to just ignore it or delete it," says Stephen Cobb, senior security researcher at ESET, a company that makes antivirus and Internet security software for businesses and individuals worldwide. "I think blocking is an option if you're getting messages from the same source all the time, but the smarter criminals will rotate the numbers they come from."

Read on for a list of some of the different types of smishing attacks you should be aware of.

The "acquaintance" you never met

Some scammers act like someone who appears to know you and lure you in with a friendly message. *USA Today* reports that the message may look like this: *Beautiful weekend coming up. Wanna go out? Sophie gave me your number. Check out my profile here: [URL].* Smishing attempts try to use common names like Don or Ann that aren't too obvious or hard to pronounce because they want to maintain their not-so-suspicious facade.

Your package is pending

Getting a text message saying that you have a package waiting for you might seem tempting, but think before you click on anything. A new text message scam has been making its way around the country. People have reported receiving messages saying: *[Name], we came across a parcel/package from [a recent month] pending for you. Kindly claim ownership and confirm for delivery here*, and then a link. Clicking on the link and inputting personal information potentially allows cybercriminals to steal your identity, empty your bank account, or install malware on your phone.

Your bank is closing your account

Cyber hackers often disguise themselves as trusted institutions like your bank or utility company to sway you into giving up your password, PIN, or other personal credentials. The message may read something like: *Dear customer, Bank of America is closing your bank account. Please confirm your PIN at [URL] to keep your account activated*. Messages of this nature also contain urgent language such as "If you don't reply within 24 hours, your account will be closed." Cobb says it's best to go directly to the company that is purporting to send you this scary message. It may require a call to your bank, but at least you'll have confirmation from the source that your personal credentials are safe.

You've won a major award

Everyone loves to win prizes—unless it's a smish prize, which is more of a win for the hackers and a loss for you. Often times, this type of text will be written as: *You've won a prize! Go to [URL] to claim your $500 Amazon gift card*. If you don't remember entering a contest for anything, do *not* click on the link, or you may inadvertently be going to a link that downloads malicious code like malware onto your phone, which can damage or disable your phone.

The bottom line: Don't click any suspicious links

The links in smishing scams often contain malicious code that can encrypt your files and lock your phone. If that happens, smishers essentially hold your phone hostage and will demand money in return for access back into your phone. The code may even give them access to all of your personal online accounts. "The text component is important because a lot of accounts we have now are using a text code to authenticate you," says Cobb. If the bank or Amazon asks for the text code they sent you to authenticate your identity, the hacker could intercept that code and access your account remotely. "It's also a good idea to update your phone to the latest operating system," says Cobb. "Most of the operating system upgrades for smartphones include security improvements."

An additional precautionary step to safeguard your phone is to install a reputable app or software that's made for mobile device protection. .

Sources:
Reader's Digest, Ashley LewisUpdated: Nov. 29, 2021. Originally Published: September 02, 2020