First Bank & Trust Company

The Bank That Puts You First

Member FDIC

April 2021 Issue 4

Romance Fraud Schemes Target Seniors

The internet makes finding love extremely easy, especially for seniors. Finding companionship online for this age group, may be a less daunting way to meet new people but it also comes with some major security risks.

Each year fraudsters use new tricks to take advantage of retiring baby boomers as well as older Americans, and using "love" as a tactic has been extremely profitable for them. Every year, millions of seniors fall victim to romance fraud, with financial losses reported to be approximately three billion dollars annually according to the FBI. In this scheme, the criminal poses as an interested romantic partner on dating websites or social media. He or she will use fake photos and create phony profiles. In some cases, they even steal the identities of real people to create accounts. The criminal then reaches out to their victims either through instant or direct messaging on the dating sites or via social media. Over time, the criminal starts to build trust with their victim, and uses that trust to capitalize on the elderly victim's desire for companionship. Unfortunately, many are persuaded to provide personal and financial information, give money or buy expensive gifts or even launder money unknowingly.

Elderly women and those who are recently widowed have shown to be the most common victim of this type of cybercrime. In 2018, the FBI issued the IC3 report, which listed confidence/romance fraud as the seventh most commonly reported and the second most costly scam in terms of complaints received and victim loss. According to the FBI, seniors are often targeted because of their financial stability and the likelihood of them having financial savings and good credit. The reports also showed many victims reported paying these scammers through wire transfers or via gift cards.

Continue on Page 2

Member FDIC

EQUAL HOUSING LENDER

Virginia Bank Locations
Abingdon, Virginia, East
276-628-3838
Abingdon, Virginia, West
276-628-9558
Blacksburg, Virginia -
540-951-1656
Bridgewater, Virginia
540-246-0003
Bristol, Virginia, East
276-466-9222
Bristol, Virginia, West
276-669-1122
Christiansburg, Virginia
540-260-9060
Fairlawn, Virginia
540-633-3793
Hanover, Virginia
804-550-5700
Harrisonburg, Virginia
540-434-0671
Lebanon, Virginia East
276-889-3401
Lebanon, Virginia West
276-889-4622
Lynchburg Virginia
434-455-0888
Norton, Virginia
276-679-7401
Staunton, Virginia
540-885-8000
Verona, Virginia
540-248-7700
Waynesboro, Virginia
540-943-5020
Wise, Virginia
276-328-3439
Woodstock, Virginia
540-459-7228
Wytheville, Virginia
276-228-1125
Operations Center
276-623-2265

Tennessee Bank Locations
Bristol, Tennessee
Volunteer Pkwy
423-652-2022
Gray, Tennessee
423-467-9966
Johnson City Tennessee
423-975-9900
Kingsport, Tennessee
423-246-3700

First Bank & Trust Loan Production Offices
Bedford, Virginia
540-583-5458
Lynchburg, Virginia
434-509-0444
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex
276-227-0722
Morristown, Tennessee
423-616-0486

First Bank & Trust Mortgage Lending Division
Bristol, Virginia
276 -644-9900

Everyone must be extremely careful when using the internet. Here are a few tips for avoiding romance scams:

⇒ *Be extremely careful about what you post online. Scammers use details shared on social media and dating sites to gain more knowledge about you.*

⇒ *Never send money or gifts to anyone you have not met in person.*

⇒ *Never give or send money or gift cards, or wire information to unverified businesses.*

⇒ *Ask lots of questions, especially if the responses seem vague.*

⇒ *Search your new companion online to verify their name, email and phone number. Sometimes other people may have encountered the same fraudster and posted information online about him or her as a warning.*

⇒ *Always keep your computer anti-virus and security software and malware protections up to date.*

⇒ *Never rush into a financial decision. Seek guidance or second opinions from family members or trusted financial advisors.*

According to the U.S. Census Bureau the 65 and older population is projected to double in size in the next decade and therefore this trend is likely to continue. If you believe that you, a family member or someone you love has been the victim of senior fraud or a romance scam report it immediately to local, state, or federal law enforcement. You can also reach out to the FBI's Internet Crime Complaint Center.

Sources:
https://cybersecurityventures.com/3-cyber-fraud-tactics-targeting-seniors-and-why-theyre-so-effective/
https://www.aba.com/advocacy/community-programs/consumer-resources/protect-your-money/elderly-financial-abuse
Elder Fraud – FBI https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud
https://www.ftc.gov/news-events/blogs/data-spotlight/2019/02/romance-scams-rank-number-one-total-reported-losses

Be Aware of COVID-19 Vaccine Scams

Last year was extremely challenging, but since December the Covid-19 vaccine began to roll out to states and across the world giving everyone hope. Each month we see availability and access to the vaccine continue to grow. But cybercriminals are trying to profit off of the COVID-19 vaccine and are sparing no one. They have launched new phishing scams and are relentless with their attempts.

Phishing attacks are still the most effective ways for scammers to gain access to personal information and data. By using emails, phone calls, text messages, fake websites and even written correspondence that appear to be legitimate about COVID-19, they trick you into divulging information such as bank accounts numbers, credit card account information, social security numbers, logins and passwords.

Earlier this month, Barracuda Networks revealed that hackers are taking advantage of the campaign to get the COVID-19 vaccine and are increasingly using vaccine-related emails in targeted spear-phishing attacks. Their study found that phishing attacks increased by 12% between October of 2020 and January 2021 and has increased to 26% since then. Barracuda found the two main types of spear-phishing attacks using vaccine-related themes were brand impersonation and business email compromise. Some of the scams included receiving text messages or emails to take a survey about receiving the vaccine and providing feedback about the experience. Once the survey is completed they claim monetary compensation will be awarded. This has caused the Federal Trade Commission to issue warnings to the public about these bad actors. There have also been reports of cybercriminals creating fake websites of the vaccine manufacturers in hopes they can trick someone into entering their personal data on the scam website.

These COVID-19 related scams continue to be extremely problematic causing Google to create a COVID-19-specific section on its Scam Spotter website to help educate people on the main types of COVID-related scams. Now, more than ever, everyone must remain digitally vigilant and scrutinize every email, phone call or text message that is received from an unknown source or even a known source.

Here are a few ways to know if the email or text you received about the Covid-19 Vaccine is a scam:

- *If you received a potentially fraudulent text message or email about a post-vaccine survey, your best bet is to just delete it.*

- *If you receive an offer for early access to the vaccine for a fee.*

- *If you are asked to schedule your vaccine appointment on an unauthorized platform.*

- *If you are asked to respond immediately for a vaccine through advertisements on social media.*

- *If you get a call or text of claims of U.S. Food and Drug Administration approval for a vaccine or treatment of which you've never heard of.*

Scammers rely on the sense of urgency to trick people into giving them money and personal information. If interested in the COVID-19 vaccine, the best way to ensure people are dealing with legitimate sources is to make the calls themselves to health providers, public health departments and other trusted sources.

Any incidents of COVID-19 Vaccine schemes should be immediately reported to The FBI, The U.S. Department of Health and Human Services and or The Federal Trade Commission.

Sources:
FTC warns of 'vaccine survey' scams, because people are the worst (msn.com)
5 Covid-19 vaccine scams to watch out for (nbcnews.com)
Beware of COVID Vaccine Scams (webmd.com)
6 coronavirus vaccine scams that target your money and personal information - and what to do about them - CNN