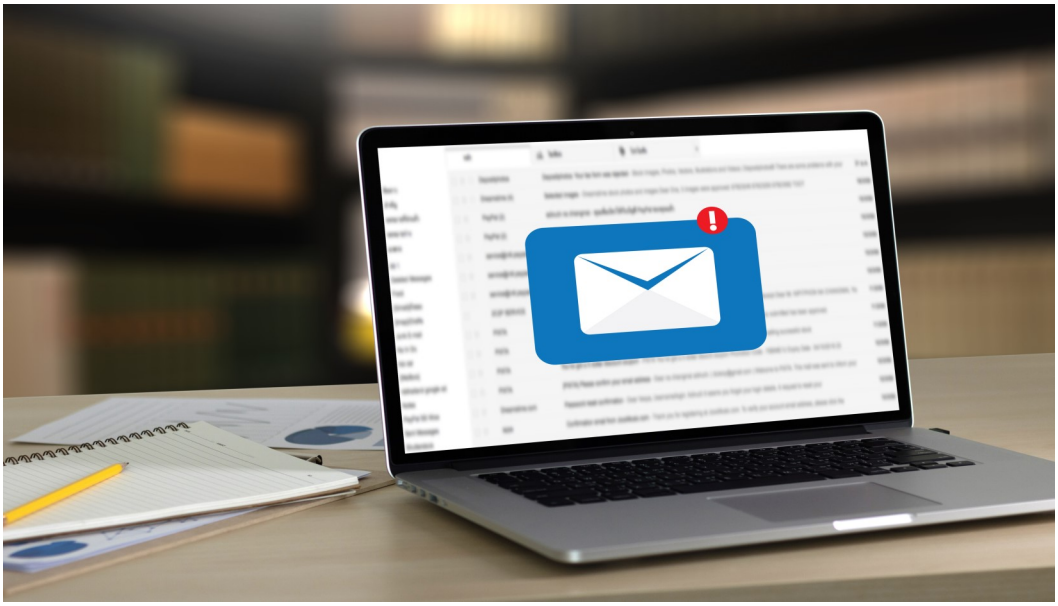
First Bank & Trust Company
The Bank That Puts You First
Member FDIC

July 2021 Issue 7

# E-Card Scam



We are living in a digital age where everything is done online. From grocery shopping to gift cards and now even greeting cards. Doing everything online is so common now that when we get a birthday e-card, a nice poem, or a beautiful virtual bouquet of flowers in our email, we don't even think twice about clicking on it. But watch out-it might be a scam!

Who doesn't want to brighten up their day with an unexpected e-card of well wishes? But not all surprises are a nice one. E-card scams are one of the latest trends that can make you a victim of identity theft or you can even lose out financially.

The spring and summer season is prime time for these types of attacks. Graduations, Mother's Day, Father's Day and birthdays are all fun events and holidays to celebrate. Cybercriminals take advantage of these days and tailor their scams to coincide with them because the likelihood they can con someone into clicking on an e-Card is very high.

So how does the e-Card scam work? It usually starts with a message sent via text, email or even direct message through social media. The message will tell the recipient they received an e-card from someone. They patiently wait for the victim to click on the link. Once clicked on, the victim might be surprised to find an empty card. But not so fast, that link could have installed malware on your computer. Once the malware is on your device the scammer can wreaking

*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
Daleville, Virginia
540-966-7006

Hanover, Virginia
804-550-5700
Lynchburg, Virginia
434-509-0444
Mount Airy, North Carolina
743-212-2013
Red Oak, North Carolina
252-220-4208
Roanoke, Virginia
540-774-0269
Rocky Mount, Virginia
540-484-0338
Winchester, Virginia
540-545-8110
Wytheville Annex

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

havoc. This access gives them data to not only the victim's personal data, but they now will have access to the victim's contacts which provides them with more targets.

It is imperative to warn moms, dads, grandparents, new graduates or anyone else celebrating a special occasion to stop and think before they click on an e-card. Pay attention to the message and look out for certain signs that may tell the e-card received might be a scam.

- *Always check who the e-card is from. Delete any e-card that does not have a real name associated with it or a name that you know.*
- *If the sender is someone you know, always verify they did send it before opening the link.*
- *Make sure you have an anti-virus/ anti-malware installed on your device.*

Scammers are hoping that you let your guard down. These days we must be more vigilant when it comes to cybersecurity. Receiving a legitimate e-card can be fun, but it's important to know the signs of e-card scams and how to protect yourself.

*Sources:*
*Online E-card Scam Greetings Give Crooks Access to Personal Data - AARP Bulletin*
*Gift Card Scams | FTC Consumer Information*
*E-card scams: Moms, dads, and grads, beware of the singing cat (norton.com)*

# Protecting Your Data From Cyber Threats


Every day, cyber security professionals are tasked with protecting data and coming up with new ways to prevent cyber-attacks; but the burden can no longer solely be left up to cyber experts. Every individual that accesses and uses data plays a part in protecting that data. The well-publicized ransomware attack on Colonial Pipeline has everyone thinking about what more they can do to be more prepared for, not if they get attacked, but when.

Today 71% of the American workforce has gone remote. This means more than half of businesses are more vulnerable than before. Unfortunately, smaller businesses are more impacted than others because they usually lack the security needed to help fight against cyber criminals. Forty-three percent of cybersecurity threats globally target small businesses. A recent survey conducted by VpnOverview found that key elements of protection were missing in smaller businesses, remote workers and ordinary consumers, the main one being two-factor authentication. The survey found that the use of two-factor authentication and VPNs (Virtual Private Networks) increased based on the size of the company. That same survey also revealed:

- Businesses with under 50 employees reported relying most often on secure Wi-Fi networks (48.3%) and antivirus software (48.3%).
- 32% of remote employees have been targeted by a phishing/cybersecurity attack more than once.
- Over two in five remote employees have experienced data breaches and/or related repercussions after experiencing a cybersecurity attack.
- 48.3% of remote employees had been the target of a phishing/cybersecurity attack at least once.
- Over 40% of these remote employees experienced data breaches and/or related repercussions as a result.

What is more important now than ever before is protecting your data. Here are a few tips to help keep your information secure:

⇒ ***Always use a VPN (virtual private network)*** - A VPN protects your information and makes it look like you're browsing using a computer somewhere else.

⇒ ***Check your privacy settings*** - Many times you leave a digital trail, especially when using platforms such as Facebook and Google. Most companies let you choose what should or should not be shared and others. Managing your privacy settings on the different sites you visit you can limit who can find your contact information and allow or not allow your profile to show up on search engines.

⇒ ***Check Permissions*** - Most apps and browser extensions have a list of permissions that you sign off on when you start using that service. Sometimes certain apps require your permission in order for them to work; for example, a maps app needs to access your location in order to provide you with the data needed. However, not all apps need to have access to your information. Double checking the permissions could prevent your data from being shared unnecessarily.

*Sources:*
*5 Tips To Protect Your Data From Increasing Cybersecurity Attacks (forbes.com)*
*https://www.forbes.com/sites/bryanrobinson/2021/06/10/5-tips-to-protect-your-data-from-increasing-cybersecurity-attacks/?sh=675f56453604*
*https://vpnoverview.com/news/how-companies-value-cybersecurity-for-remote-employees/*