Avoiding Coronavirus Fraud and Phishing Scams

FIDUCIARY™ TRUST

Information Security Insights

April 29, 2020

Throughout the digital age, bad actors have expanded their use of various channels to pursue financial victims, including email, websites, phone calls, text messages, and links in social media posts. Unfortunately, the COVID-19 global pandemic has led to an uptick in related phishing activity.[1,2]

The fraudulent attempt to gain sensitive information such as usernames, passwords, credit card numbers, or social security numbers for financial gain is often referred to as "phishing," a homonym of the word "fishing." Another threat is malware, which is malicious software that can be installed on a computer or mobile device without consent. Criminals will use malware to steal personal information, send spam, or commit fraud.[3]

Below are a couple of key principles to help protect your identity and examples of recent phishing activity and scams to heighten your awareness of these schemes.

Exercise caution when clicking on links

Email links. Avoid clicking on links in emails, texts, and other online locations from unknown sources. Do not assume that emails or text messages purporting to be from people or organizations that you know are actually from those people or organizations. Their email accounts can be "spoofed." Spoof emails are sent by a malicious third party and can be made to appear as if they are coming from a legitimate source.

Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

Rick Tyson
tyson@fiduciary-trust.com
617-292-6799

Be careful when clicking on email links

For example, be careful when clicking on email links that supposedly come from a financial firm, as scammers can create emails that appear to be coming from legitimate companies. Links from scammers may take you to a site that looks like your bank's website and ask you to type in your login credentials. However, they are actually stealing your credentials to log into the site for themselves. A better practice is to go directly to your institution's website by typing the address in your browser, which you know it is legitimate, or using your institution's mobile app.

One way to reduce your risk is to check the hyperlinks in an email that appears to be from a reliable source. You can do this by hovering your cursor over a link without clicking on it. The link address will appear and allow you to confirm that the URL website address matches a reliable site. For emails from Fiduciary Trust, the links will start with "fiduciary-trust.com," "go.fiduciary-trust.com," or "fidtrustco.com." Capitalization does not matter, but you should be on the lookout for minor URL variations, and also beware that the URL as it is written in the body of an email may actually be different from the URL to which the link will send you. A potential red flag to check for is whether the URL in the email is different from the URL that appears when you hover over it with your cursor.

Website links. If you are on the website for a reliable source, such as fiduciary-trust.com, you should not have to worry about clicking on site links, unless something appears blatantly suspicious. Note that bad actors can copy entire websites, but they cannot duplicate the URL, so when in doubt, it is wise to check the URL.

Limit disclosure of sensitive information

As a rule, do not directly respond to requests for information unless you are absolutely certain of the source. If someone calls you from an organization with which you do business, but you are not certain that the person is legitimate (i.e., you don't know them by voice), then hang up and contact the organization using a number or email that you know is legitimate. A similar point applies for emails. Whenever you are in doubt about the authenticity of a communication, a safe protocol is to reach out to the person or company directly to ensure the request or information is legitimate.

A good general principle to follow for phone calls is to **let callers from unrecognized numbers leave a message**. If the topic is important enough, the caller will leave a voicemail. And often, the information left on that voicemail can go a long way in allowing the person to identify whether the call is legitimate, or a scam.

Avoid sharing sensitive information unless it is through a secure channel to a confirmed source, such as Fiduciary Trust's secure email service, or by speaking with a Fiduciary Trust employee with whom you are familiar.

Legitimate organizations will never contact you for your password or Social Security number. Social Security numbers are typically only used when opening accounts at financial institutions, creditors (including landlords or utility companies), or starting a position with a new employer.

Examples of phishing attacks

Coronavirus

Scams that the Federal Trade Commission has warned consumers about[4] include:

- **Offers for COVID-19 vaccinations and home test kits**
- **Illegal sales calls** designed to obtain money and personal information from unsuspecting victims
- **Phishing emails and text messages** purporting to be stimulus checks from the government, Medicare benefits related to coronavirus, and the **World Health Organization (WHO)** or the Centers for **Disease Control and Prevention (CDC)** calling to collect information.
- **Fake CDC Alerts** – Scammers have been sending emails claiming to be from the CDC. These emails may say that the CDC has a list of people in your area exposed to COVID-19, and encourage you to click a link to review these names.

  Some indicators that these communications are not legitimate are: First, the CDC would not have your email, or contact you via email if it thought you were exposed. Second, it is illegal to reveal an individual's health status, so you would certainly not be provided with someone's name, let alone their health status.
- **Heath scams** – Some emails purport to have a cure or a vaccine – you just need to send some personal information and they will send it to you or have someone contact you. If a treatment or vaccine is made available, it will not be announced via email. The websites for the CDC, the WHO, and the National Institutes of Health (NIH), listed here, are all good sources of information about the virus: **CDC**: www.cdc.gov, **WHO**: www.who.int, and **NIH:** www.nih.gov.
- **Charitable giving** – The Federal Trade Commission also recommends that consumers do their homework when it comes to making charitable donations, and never make donations in cash, by gift card, or by wiring money.
- **COVID-19-tracking websites** – Scammers have set up websites to purportedly help track the spread of the virus. Instead, they will ask for your personal information that will help them try to either guess your passwords or security questions, or social engineer their way into your accounts.
- **Remote work scams** – If you are working from home due to the coronavirus, scammers may pose as your company's IT helpdesk and request that you download files to access your corporate network. Before downloading anything, contact your firm directly at a phone number you know (not one from the email or message you just received) to confirm. It is likely that the file they are sending you is malware, which can send them information from your computer on an ongoing basis.

Scammers have been sending emails claiming to be from the CDC

Census 2020

Census 2020 scams include fraudulent attempts to gain sensitive information under the purported guise of the census, whether via mail, email, or in-person solicitation. However, one should know that the Census Bureau will never ask for Social Security numbers, bank or credit card numbers, or for any money,

donations, or anything on behalf of a political party. The bureau also will not send emails unless you have signed up to receive them.[5]

Social Security

There are several common Social Security scams. In one version, a caller claiming to be from the Social Security Administration (SSA) will use threats – such a warrant or imminent arrest – to induce a state of fear and then ask for a payment, often in the form of gift cards, which can be difficult for authorities to recover.

There are several common Social Security scams

Other scammers will tell victims that their Social Security number has been suspended because of suspicious activity, or because it has been involved in a scam.[6] They will ask the person to confirm their Social Security number or to withdraw money from the bank. Often they will threaten to seize or freeze the victim's account if they don't act quickly.

Criminals employing this tactic often use robocalls to reach people, and leave messages that seem hard to ignore. They can use a caller ID spoof to make it look like the real SSA is calling. However, the SSA will always send a letter first.

On a related front, one protective step you can take is to set up your My Social Security account. Regardless of your age, establishing a My Social Security account makes it more difficult for someone to access and compromise your Social Security number with the SSA. You can set up your account by visiting www.ssa.gov/myaccount. Since the SSA site may use information from your credit report to confirm your identity, you should ensure you do not have a freeze on your credit report when setting up the account.

IRS Imposter Scams

A precursor to the Social Security scam, this often involves threatening phone calls designed to illicit fear and obtain sensitive personal information. Keep in mind that the IRS will not call you and ask for your bank account information. The IRS either already has your information or will contact you via physical mail.

Computer Security Updates

Tech support scams can involve calls or, more often, computer pop-up windows. The pop-up windows will look like an operating system error message or antivirus software. These can often look very realistic with logos from trusted companies or websites. The message will warn of a security issue on your computer and ask you to call a number to reach a live technician. Next, this live "technician," will try to get you to pay for "tech support" that you do not need, ask for remote access to your computer, or for your usernames and passwords.[7]

A variation of this involves a person calling to offer a refund for technical support, however, in either scenario, these thieves are trying to steal money.

"Grandparent" Scam

Targeting older adults, scammers will call claiming to be the person's grandchild, stating that they need bail money, money for a medical bill, or are in some other trouble requiring money, and ask you not to tell anyone. These scammers can be surprisingly convincing, and may utilize personal information from a hacked email account. If this happens to you, stop to check it out, call the grandchild directly, or ask another family member.

Author

Robert J. Jeffers
Chief Operating Officer

Learn More:

For more insights or information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

Rick Tyson
tyson@fiduciary-trust.com
617-292-6799

Social Media Scams

Some "quizzes" on Facebook will ask for information often used as online security questions, such as a high school mascot or childhood best friend. Another kind of social media fraud are "romance scams," in which a perpetrator pretends to be romantically interested in the victim. However, their real purpose is only to cheat them out of money.

Moving Forward

As general guidance, it is important to be particularly vigilant during this difficult time, as unfortunately, scammers are trying to take advantage of people. Go to your financial institutions' websites directly, do not give out personal information to someone you do not know, and remember that if something sounds too good to be true, it probably is.

The Federal Trade Commission encourages consumers to report all scams, including coronavirus-related scams, via its website FTC.gov/complaint, which also helps other people. The website includes information on many other types of scams, and sample emails and recorded phone messages from scammers, so consumers can double-check on inbound solicitations they believe may be suspicious.

Fiduciary Trust takes information protection seriously and employs a number of safeguards and ongoing testing to help keep client and other information secure. We have additional resources available in our related articles "Protecting Your Identity" and "Cybersecurity: Reducing Your Risk." ■

[1] https://www.consumer.ftc.gov/blog/2020/04/scammers-are-using-covid-19-messages-scam-people

[2] https://www.ftc.gov/system/files/attachments/coronavirus-covid-19-consumer-complaint-data/covid-19-daily-public-complaints.pdf

[3] https://www.consumer.ftc.gov/articles/0011-malware

[4] https://www.consumer.ftc.gov/features/coronavirus-scams-what-ftc-doing

[5] https://2020census.gov/en/avoiding-fraud.html

[6] https://www.ftc.gov/news-events/blogs/data-spotlight/2019/04/growing-wave-social-security-imposters-overtakes-irs-scam

[7] https://www.consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

FIDUCIARY™ TRUST