Maximizing Email Security

FIDUCIARY™ TRUST

Information Security

In modern life, and especially during the COVID-19 pandemic, Americans rely on digital communications to manage everyday affairs, including personal banking. Unfortunately, that dependence on technology has left some Americans vulnerable to various forms of cyberfraud. Over the past several months Fiduciary Trust has seen an increase in reports of hackers gaining access to clients' email systems, and we want to inform you about them.

Cybercriminals have been obtaining email passwords by exploiting weaknesses in common websites and carrying out so-called social engineering attacks. After hackers access an email account, here are several tactics they use to defraud individuals and siphon their funds:

1. Review your emails to find bank statements and potentially reset your passwords
2. Send emails to your friends and relatives asking for money
3. Mimic your previous email requests for cash transfers, and ask your banker to direct more money to an account

At Fiduciary Trust, we have encountered the third tactic often enough to warrant a word of caution to our clients. Know that we use strict call-back procedures to protect our clients from that particular scam. We will not move money without getting verbal authorization from you directly. Many firms might honor a request to move money if the instructions come from a client's email address, but we will take the extra step to verify that the request is authentic.

Learn More:

For more information on Fiduciary Trust visit:

www.FidTrustCo.com

or contact:

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

Author

Robert J. Jeffers
Chief Operating Officer

For individuals with accounts at firms that allow online transfers, hackers illegitimately resetting passwords on financial accounts is of particular concern. (Note: Fiduciary Trust does not allow online funds transfer via client accounts.) Once inside an individual's email, cybercriminals can root out electronic statements, log on to the bank's system, click "forgot password," and obtain a reset password link. With access to a client's email and bank accounts, the hacker then has full control of their funds at that firm.

Fortunately, you can protect yourself with a few easy techniques:

Use A Unique Email Password – Your email password should be completely different from all other passwords, especially ones that you use online. The easiest way for hackers to gain access to your email is to actually hack another, less secure site, like one for a local meetup group. Websites that do not manage financial transactions or involve other private information have low security thresholds. Unfortunately, the username on these sites tends to be your email address. If you use the same password on that site as you use for your email, you have essentially given the hacker access to your account. While all passwords should be different, it is imperative that your email password is secure and unique, because it is a potential gateway to other online accounts.

Choose Two-Step Verification – Also known as multi-factor authentication, this can be used to protect your email account. All major email providers allow you to opt into a two-step verification. After you enter your password to log in, your email carrier can send a code to your phone – usually numerical – that you type in to get access. You only need to do this the first time that you use a single device. Using two-step verification, even if someone gets your email and password, they cannot get in, because they will not have access to the code that is going to your phone.

Avoid Social Media Polls – While the polls on social media sites like Facebook asking you to name your favorite movie, pet's first name, or first concert may seem harmless, many of them are a sophisticated form of cybercrime called social engineering attacks. In some cases, these so-called pollsters are trying to gain personal information about you, attempting to guess your password. It is best to ignore them.

Fiduciary Trust understands that our clients' computers and mobile devices have helped make everyday tasks easier to manage. It is very important, therefore, to maintain secure access to financial communications. Please consider taking the steps above today, as a way to better protect your information. ■

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

FIDUCIARY™ TRUST