BAIRD

Private Wealth Management

Cyber Self-Defense: Protecting Yourself Online

If you're like most people, you spend a considerable amount of time on the Internet. According to data from USC Annenberg, Americans spent an average of 24 hours per week online in 2018. If you're reading this article, you're online right now.

Criminals are also spending more time online, trying to steal everything from our money to our identities, and our increased comfort level with online services and social media have created many ways for them to do that. These scammers aren't just targeting older people who might be less tech-savvy. In 2018 the Federal Trade Commission revealed that "of those people who reported fraud and their age, 43% of people in their 20s reported a loss to that fraud, while only 15% of people in their 70s did."

Here are some of the most common scams going around the Internet now and how you can protect yourself from them:

FAKE SOCIAL MEDIA REQUESTS

Facebook and other social media platforms can send you emails with activity updates and new friend requests. So can scammers, and theirs can look just like the official ones. In an ironic twist, sometimes the scammers will send an email warning that someone has been trying to access your account. Whatever the message, the goal of these fake social media emails will be to get you to click a link that takes you to a fake login page in hopes to capture your credentials. Signing in on that bogus page allows the scammers to hack into your actual account.

What you should do:

Never click on any links that are emailed to you unless you're sure who sent the link and where it goes. Always go to your social media pages by typing the Web address into the URL bar or opening the social network's app on your phone. Better yet, set up two-step verification on all of your social accounts so that ▶

Wathen Lobel Miller Schultz Group
Baird
Private Wealth Management
wlmsgroup@rwbaird.com
wlmsgroup.bairdwealth.com

signing on requires a special access code be texted to you in addition to you providing your log-in credentials.

PHISHING ATTEMPTS

More than a third of all successful cyber scams start with a phishing email. Like the fake social media request, these appear to come from an official source – like your bank – and ask you to log in to a seemingly legitimate site. Or they might ask you to reply with some private information, like a password or credit card number. Or they may tell you that you are receiving the message due to fraudulent activity on your account and ask you to "click here" to verify your information.

What you should do:

Stay calm. Many phishing scams rely on your emotional response to the prospect that something is compromised or at risk to make you react quickly. Take your time and look at the URL you are asked to click on as well as the email address of the sender. If these elements of the email don't synch up with the institution the email claims to be from, you can reach out to your bank or credit card company directly to verify the legitimacy of this email. If they haven't sent you anything, simply hit "delete."

DATING SCAMS

For busy or socially reserved people, dating apps have become a popular way to meet potential romantic partners. Their popularity, though, and the very personal nature of the information often shared on them makes them prime targets for cyber scams. A scammer might lure you in with messages, phone calls or pictures but will be reluctant to meet in person. Once they've gained your trust and learned more about you, they make their pitch – usually something to do with being short on cash. Can you help? Maybe wire them some money?

What you should do:

Unless you're donating through a reputable charity, you should never give money to someone you haven't met in person. And anyone you connect with on a dating site who doesn't want to meet you in person almost certainly has other motives for being there.

FAKE ANTIVIRUS SOFTWARE

Another ironic and particularly annoying scam starts with a message that pops up on your computer or smartphone screen, usually while you're trying to navigate somewhere: "Your device has been infected!" And the only remedy is to "click this link to run a diagnostic" or "download this antivirus software."

The most benign outcome of clicking that link is typically malware that plants unwanted pop-ups on your screen while you browse online, which can be pretty irritating. A far worse scenario, though, is ransomware. This kind of attack can block your operating system from working at all until you send a sizable sum of money for the "antivirus system," which is just a decryption key.

What you should do:

The most important thing, of course, is to resist clicking on any hysterical warnings. Close your browser windows and reopen them. If the message reappears, restart your device. New versions of this kind of attack are being invented all the time, so make sure your real antivirus software is up to date and active.

MAKE MONEY FAST SCAMS

The digital-age version of this time-tested scam might pop up in your feed promising the secret to making thousands of dollars just by being on Facebook all day. One of the most common versions claims you can make hundreds a day by posting ads on Facebook. But if you dig in, you'll find what they're offering is a how-to for posting essentially the same kind of ad that snared you – promising other users the secret of making money on Facebook – and all this invaluable knowledge will cost you is just a small fee.

What you should do:

Never send a stranger money, on the Internet or anywhere else, until you're sure of exactly what you're getting in return. And if what that stranger is selling doesn't sound like anything you would be interested in offline, the fact that it's on Facebook doesn't make it a better idea.

GREETING CARD SCAMS

Greeting card scams are similar to the fake antivirus scams in that they're designed to put malware on your hard drive. You'll get an innocent-looking email notifying you that someone has sent you an electronic greeting card. The idea is that once you open the email and click the link to see the card, malicious software is downloaded and installed in your operating system. You may start to get constant pop- ▶

Cyber Self-Defense: Protecting Yourself Online *continued*

up ads, or even worse, your computer could start sending private data and financial information to the scammers.

What you should do:

Never click a link, open an attachment or download anything from an unknown source or sender. In this specific case, ask yourself why someone you don't know would send you a card.

All of us at Baird take your financial security seriously. Contact your Baird Financial Advisor for information on how we keep your private information secure.

Please reach out if you or anyone you know would benefit from discussing this topic further.

Find additional financial planning content on BairdWealth.com.