Second Quarter 2021

Online Threats from Scammers Are Booming

Over the past year, the email IN box has become an even greater minefield of threats to your financial welfare. It is a rare internet user who has not received:

- Threats of service cutoffs if payments are not made immediately,
- Invoices for products you never ordered,
- Sproofed emails from friends asking if you know who is in the attached image
- Requests for help making an Amazon purchase,
- SBA applications for pandemic loans,
- Notices of suspicious activity in your accounts that need to be verified,
- And more and more increasingly sophisticated scams.

Sometimes the scams are conducted through phone calls and, less frequently but still occurring, direct mail. The most effective often use a technique called “spear phishing,” including details about one’s personal life and relationships to make the recipient think the messages are 100% legitimate. Where do scammers get their information? Typically, from their victim’s online postings. We share far too much information about ourselves online, warn fraud prevention experts.

- Online dating sites have also become a favorite of predators. Think your identification is confidential? Try a reverse image search on Google using your photograph and see what results you get (Go to images.google.com, click the camera icon, and either paste in the URL for an image you've seen online, upload an image from your hard drive, or drag an image from another window). Reverse image searches are also available on Bing and Chrome search engines. Armed with your name, a predator can look up other details, including work, hobbies and more, and use that information to create a persona that seems your perfect match. If you have questions about someone who says they know you, try a reverse image search on their photo. It may turn out to be a standard model shot or even someone altogether different.

Where do you start with protecting yourself from fraud?

1. **Limit information about yourself online.**

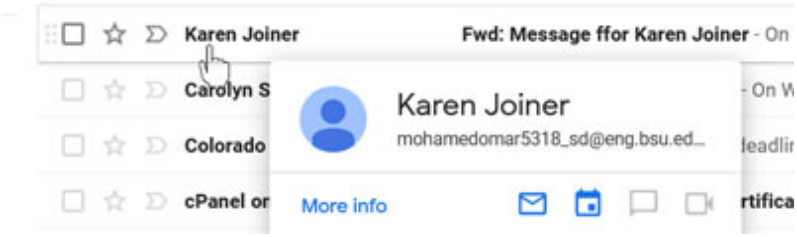
   There is no need for your online professional profile to include hobbies, mentions of your children or spouse. Don’t have Facebook friends you do not know personally. Limit information about you on business databases that could be used if the database is breached.

2. **NEVER EVER provide confidential information such as passwords, credit card or bank account information, social security number or even your address to an email address or online link included in an email or to a phone caller.**

   Log in direct to any accounts (retailers, social media, bank, credit card provider, etc.) that appear to be seeking that information, check your messages, and report the fraud.

3. **Verify the sender before opening any email attachments or links.**

It is very easy to “spoof” or fake an email address. It is less easy to hide the information from a “scroll over” of the address or the address that shows up if you reply to the email. To scroll over an email, hover your cursor over the email address. The image below shows how an address scroll over appears on Gmail. In Outlook you can find additional information on the email by clicking FILE, then PROPERTIES.



4. **Check the URL of any links in the email**.

If you place your cursor on links within the email, Gmail shows the actual url at the bottom of the screen. Outlook opens a box with the link address. Don’t click on links in an email without first checking where they will take you. And don’t assume that a secured https: site is safe. The Anti-Phishing Working Group reports that 35% of all phishing sites were using HTTPS and SSL certificates. With Google now labeling non-HTTPS website as “Non-Secure,” expect to see more phishers abuse the accepted concept that HTTPS sites are trustworthy and legitimate.

Double check the legitimacy of any communication with a friend or by phoning the government organization or business before opening attachments or clicking links. This is your best protection. When it comes to contacting the organization, NEVER dial the number found in an email or left on a voicemail, as it could be fake. Search online for the organization for its correct contact number.

This information barely touches on the extent of email and internet fraud that exists today. And when it comes to fraud, you are on your own. There’s no anti-fraud insurance or government agency to protect you from a mistake. Once your money is gone, it’s gone. In the end, you have to protect yourself through what may seem like an excess of caution but is very necessary. The more you can learn about protecting yourself from email cons, the less likely you are to pay for a costly mistake.

TOP

Brian R. Carruthers, CFP, CMT

BCA
BRIAN CARRUTHERS & ASSOCIATES

Your Conservative Advisory Firm Since 1990
301 Forest Avenue
Laguna Beach, California 92651-2115 USA
Telephone: 1-949-464-1900

www.gobcafunds.com
brian@gobcafunds.com