INSIGHTS

Cyber made simple.

one brightly cyber

CYBER SCAMS

BY JAY BORDEN

Attackers are clever and use many different approaches to fool people. Of course, their only goal is to get you to click a link or get private information another way. Attackers are getting better at fooling people and Artificial Intelligence, AI, aids them in creating scams that can fool almost anyone.

Some examples of recent scams including ones enabled by AI.
You receive a call from a relative saying they lost their wallet or are in trouble and need money wired immediately. With just a few words spoken by a person AI systems can create realistic messages saying anything that sounds real.

It's not difficult to get a sample of someone's voice. It may be they gave a talk posted online. Or they were at a party with videos posted. Or their voicemail.

The request for immediate action is a red flag. If you can't call the person, call their family members, friends, business colleagues or anyone else who would know if the person is away or in trouble.

Another type is a call claiming to be from your bank or the utility company or any other company you do business with. It says your account is in arrears and will be frozen unless payment is received immediately.

Again, the short time frame to respond is a red flag. Verify that the call is real by contacting the company directly. Never use a phone number or email given on that call or in an email message. Contact the company using a number you know or one on their website. The call is most probably a scam. Be sure it is real before sending money. Once money is sent electronically, it is very difficult to recover.

Who doesn't like a great deal? Especially on something you really want! Cybercriminals know this and take advantage by posting ads on social media. Not surprisingly, the ads go to sites run by the cybercriminals.

onebrightlycyber.com
(888) 773-1920

CYBER SCAMS

CONTINUED

Your credit card number will be required just like any legitimate site. Except here you are giving it to criminals. They will not care how much they spend because it will be billed to you.

A different type of scam - someone you only met on line, probably an attractive looking young woman, either asks for money or tells you about a wonderful way to make money. If they are asking for money, know it is a scam.

If it is to make money by buying and selling cryptocurrency it is a scam. They recommend an app that takes care of the timing and where to buy and sell it for you. The app has a dashboard to show your progress and will show that you have made huge profits that keep growing. Until you want to get your money. If you only want a small amount of money they will probably send it. But if you want more than a small amount, you will discover there isn't any money in your account. The criminals never bought or sold anything for you. They simply took all your money.

Another scam is a popup on your computer saying a virus was discovered on your device. Click the link to give them access to your computer and they will remove it. Never give anyone access to your computer. It's not a virus they will remove, it's your confidential information. They will install malware like keyloggers that capture everything you type including usernames and passwords.

One more, if you need to make a wire transfer for a real estate closing or any other reason and an email comes changing the wire transfer account, do not do it! Call the bank or other institution or a known contact directly using a number you know, not one in the email, to verify the change. The account number in the email or text will send the money to the cybercriminals. A phone number in the email will also go to the cybercriminals.

And another, you receive money through a payment service, Venmo, PayPal, Zelle, etc. from someone you don't know. What do you do? Do Nothing! The money you received was probably from a stolen credit card and will be reversed by the payment service. If you send money back it not be reversed as it is a legitimate transaction.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.