HBKS Wealth Advisors

Watch Out for Scammers

By Jim ARCORACI, CRPC®
Principal, Senior Financial Advisor

WE ARE IN THE MIDST OF A NATIONAL EMERGENCY. The government is offering benefits to victims; your new way of business is requiring new, unfamiliar technology, and uncertainty is driving you to new apps and websites in search of information to help you stay afloat — all of which are being seized upon as new opportunities by cybercriminals.

Criminals are scamming individuals and businesses of their money and data through myriad tricks. Current scams are related to:

- The IRS or CARES Act
- Stimulus Payments
- COVID-19
- Charitable Giving Sites
- Current Updates — Statistics and/or Heat Maps
- Early Vaccine/Treatment Access
- Problems with a Bank Account or Credit Card
- Investment Opportunities
- Blood Donation

Here is what cybercriminals are doing:

METHOD 1: MASQUERADING

Cybercriminals are exploiting the necessity for individuals and businesses to deploy new IT resources and methods to conduct work remotely such as VPNs, screen sharing technologies, and remote meeting software. Criminals are developing malicious tools that appear legitimate. Unsuspecting users, in search of a tool to facilitate their needs, instead download a malicious VPN agent. It is important to discuss any new IT resources you are considering with a professional who can advise you not only on the best, but the most secure tools.

Our current national emergency is giving cybercriminals new opportunities to scam individuals and businesses.

Also, as your business operations change, cyber criminals are waiting to involve themselves in the process. Man-in-the-middle attacks involve criminals intercepting emails detailing payment instructions and bank account numbers and re-routing them to off-shore bank accounts before forwarding the email to the recipient. The sender and recipient are none the wiser until they discover that the money is gone.

The IRS or other government agencies will never call, text or email you for payment or bank account information.

METHOD 2: PHISHING/VISHING/SMISHING USING COVID-19 THEMES

Attacks may come in the form of fraudulent emails (i.e., "phishing"), text messages (i.e., "smishing") or voice calls (i.e., "vishing"). These attacks may take advantage of users by posing as the following:

1. The IRS
2. Charitable Agencies
3. Tech Support

Remember, the IRS will NEVER call, text or email you for payment or bank account information, nor will other government agencies. Scrutinize every unfamiliar call, text, or email and avoid disclosing your personal information.

METHOD 3: FAKE MOBILE APPLICATIONS

Cyber criminals understand that we regularly download apps to facilitate our daily needs. There have been multiple cases of malicious Android applications claiming to offer information about the virus or to accommodate your business needs in these times of uncertainty. But all they really offer is attackers the opportunity to spy on you, steal information, or ransom your data.

METHOD 4: MALICIOUS AND FRAUDULENT WEBSITES

The Palo Alto Networks threat intelligence team notes that over the past few weeks more than 100,000 websites have been registered containing terms like "covid," "virus," and "corona." Many of these websites are used to deploy malicious software that can threaten your business operations and data security or trick you into thinking you are applying for stimulus loans through their interfaces. Some websites spread false information to create unnecessary action or panic. Such risks can be avoided by using only trusted sources.

Do the following to protect yourself from becoming a victim of a fraudulent attack:

- Use extreme caution when dealing with any email with a subject line, attachment or hyperlink pertaining to COVID-19.
- Be cautious when dealing with an email, text message, social media post, or phone call with a subject line or topic pertaining to a COVID-19 related matter.
- Use only TRUSTED Sources, such as known government websites, for updated information on COVID-19.

Some websites spread false information to create unnecessary action or panic. Such risks can be avoided by using only trusted sources.

- NEVER trust a hyperlink in a communication stressing urgency, such as a warning about a severe problem pertaining to financial information — i.e. bank accounts, credit cards or the IRS.
- Verify that the contact information is from a trusted source — for example, the toll-free phone number on the back of your credit card.
- If you visit a website, open it directly from your computer or a previously used app on your smart phone instead of from the requesting email.
- Never provide any identifying number over the phone, such as your Social Security number, Your Medicare ID number, your driver's license number or your bank account number.
- If you need to implement new technology or processes for your business or personal life, consult a professional.

Jim Arcoraci, CRPC®
Principal, Financial Advisor, HBKS® Wealth Advisors

As principal and senior financial advisor in the HBKS® office in Fredonia, New York, Jim Arcoraci is a principal and financial advisor in the Fredonia, New York office of HBKS® specializins in personal financial planning, including investments, retirement, estate planning, education funding, tax management and wealth preservation strategies. Jim can be reached at (716) 672-7800 or at jarcoraci@hbkswealth.com