HBKS Wealth Advisors

Phishing Scams are Everywhere: Be Prepared

By Michael G. WASSMANN, JD
Chief Compliance Officer

Cyber security threats are everywhere in today's high tech world, and simply having an email account puts you at risk from the largest and fastest growing threat, known as phishing. The reason phishing is so dangerous is that fraudsters can easily deliver their schemes directly to your email inbox through a dizzying array of believable scenarios. Recent estimates suggest more than 150 million phishing emails circulate daily, and about 16 million of those make it through email security filters to inboxes. Of those, half are opened, with nearly one million people taking the bait each day.

WHAT IS EMAIL PHISHING?

Email phishing is the use of email to present a scenario that tricks victims into providing confidential information or downloading malicious software. The fraudster then has access to your accounts or can steal your identity. Often email phishing attempts are obvious, as they contain many grammatical errors and present absurd claims. Others are clever and persuasively mimic real life situations to provoke a response. Fraudsters disguise email addresses, hide malicious links and copy company logos to appear legitimate. Given this risk, it is important to take steps toward protecting against phishing.

HOW TO AVOID EMAIL PHISHING SCAMS

An initial step to protect yourself is to arm your computer with automatically updating security software designed to identify and filter phishing emails. Good software can stop the majority of phishing emails from reaching your inbox and protect against known types of viruses. You should also backup your computer files in case you do fall prey and your files become damaged, lost or locked.

Another step is learning to identify clues so you can avoid phishing emails that make it to your inbox. When first learning to spot potential clues, it is important to understand that phishing emails generally seek to do one of two things:

- Attain confidential information: Fraudsters seek confidential information from you, such as Social Security numbers, account numbers and login information so they can access your accounts or open new accounts in your name; or

- Download malicious software: Fraudsters try to trick you into clicking on a link or downloading a document that will load a virus onto your computer.

If an email asks you to provide confidential information, click on an unknown link or download an unknown document, there is a good chance it is phishing. Other clues that an email is phishing include:

- Suspicious senders: Do you recognize the sender? Remember that fraudsters can disguise an email address, so hover your mouse over the sender's name in the email until the underlying email address appears. Do you recognize the email address? Does it match that of the sender?
- Unusual methods of communication: Does the sender normally communicate this type of information in this manner? Is this normal for the sender?
- Strange timing: Was the email sent at a strange time of day such as 3 a.m.? Odd timing can indicate an unreliable source.
- Odd grouping of recipients: If there were multiple recipients, do you know the others and does it make sense that they would be included in an email group with you? Fraudsters often group unrelated recipients to reach more potential victims with reduced effort.
- Unrelated communications: Is the email message about a subject you were not expecting? Fraudsters create false subject matter to induce a response by making claims such as undeliverable packages, overdue invoices, unclaimed prizes, security risks on existing accounts, etc.
- Poor grammar and spelling: Poor grammar and incorrect spelling often indicate the source is fraudulent, as they are often drafted in haste or come from foreign sources.
- Unusual circumstances: Are you being asked to do something out of the ordinary? If so, it may be worth additional consideration before acting.
- Discomfort in the situation: Are you uncomfortable with the circumstances? What does your gut tell you? Your instincts are often correct and it is worth your time to investigate further.
- Disjointed Content: Does the subject line of the email match the actual content? Is there just a link with no message content? Fraudsters often take shortcuts and send out thousands of poorly designed emails hoping that a few recipients will simply click on links out of curiosity.
- Urgency: Does the email present an urgent situation to put pressure on you to act quickly? Examples include claiming an imminent account suspension, overdue invoices, threatening legal action, government penalty or offering a prize that must be claimed immediately. Fraudsters rely on urgency to encourage impulsive responses.

- Government threats: Is the email supposedly from a government entity? Government entities rarely use email to make initial contact regarding enforcement matters. The IRS will never use email to contact you.
- Unknown links or documents: Are you being asked to click on an unfamiliar link or download a document? Hover your mouse over the link or document button so that the underlying link appears. Does the actual link match the subject matter of the email? Is the link suspicious? Watch for similar, but slightly different spellings in the web address.

These are only some of the clues indicating that an email may be phishing. As fraudsters develop new techniques, other red flags will emerge, and you should remain diligent when considering whether any given email is phishing.

HOW TO RESPOND TO KNOWN OR SUSPECTED PHISHING

If you have determined or suspect that an email is phishing, it is crucial you do not provide any information, click on any links or download any documents. If you know it is phishing and your email system allows, mark the email as spam or phishing in order to block all future emails from that email address and then delete the email.

If you are uncertain as to whether or not an email is phishing, find an alternate way to communicate with the supposed sender to check out the email. If it is from a friend, call them or text them to confirm. If it is from a business, call them at a phone number from another source such as the back of your bankcard, the internet or yellow pages. Do not rely solely on a number provided in the email. Visit a local branch if possible. If the email claims a problem with your online account, close the email and log into your account using your web browser and determine whether there is a problem. If you cannot ascertain if the email is phishing, do not act on the email and treat it as if it were dangerous.

WHAT TO DO IF YOU BELIEVE YOU HAVE FALLEN PREY TO PHISHING

If you think you have fallen for a phishing scheme by providing confidential information or clicking on a link, there are important steps you can take to protect yourself.

- Protect your accounts: Contact banks, advisors, brokers, custodians, insurance companies and other entities holding your assets to look for unusual activity and discuss steps to protect against identity theft, including available heightened security procedures.
- Update passwords: Change your passwords on your accounts and electronic devices using complex passwords. Keep in mind that if you have provided login information or downloaded malicious software the fraudsters could have access to any information on your computer, and may be monitoring your key strokes.
- Credit monitoring and credit report locks: Consider setting up credit watch services that monitor the credit rating companies and any attempts to open accounts in your

name. You may also set up credit locks with the credit rating companies to discourage anyone from getting credit reports needed to open accounts in your name.

- Have an expert check your computer: Hire an IT expert to check your computer for malicious software, and confirm your cyber security protection software is up-to-date.

Many other steps can be taken in response to actual or potential identify theft. Visit identitytheft.gov to see what you can do, and how to develop and implement a recovery plan.

Please remember that information provided here is not exhaustive. There are countless and ever-evolving email phishing schemes. Your best defense is to be attentive and diligent, remaining cautious at all times.

Important Notice: While security software and diligence are important steps in protecting against phishing, there is no guarantee that following all of the steps, and considering all of the factors, contained herein will allow you to protect against all phishing threats. Fraudsters using phishing are always changing their strategies, and are clever and determined. There exists fraud strategies not covered by this document and new fraud strategies will be developed in the future, which are not addressed. As such, there is always a risk of falling prey to phishing. The information in this document is presented for informational and educational purposes only, and HBKS Wealth Advisors does not guarantee that following all steps and considering all factors in this document will protect you from phishing attacks. In addition, protective measures discussed herein must be implemented by you, and HBKS is not responsible for applying those protective measures on your behalf.

Michael G. Wassmann, JD

Chief Compliance Officer, HBKS® Wealth Advisors

As the Chief Compliance Officer, Mr. Wassman ensures that business is conducted within the guidelines set forth by various regulatory bodies. He works out of the Erie, Pennsylvania, office of HBKS® Wealth Advisors.

Michael joined HBKS in 2011 and has 26 years of legal experience that includes both private practice and in-house counsel work. His private practice involved complex litigation in the areas of state and federal regulation of financial services and consumer protection. His in-house practice work included acting as both Chief Compliance Officer and General Counsel for financial services companies.

Michael has practiced law in Michigan Circuit Court, Michigan Court of Appeals, U.S. District Court for the Eastern District of Michigan, U.S. District Court for the Southern District of New York and the U.S. Court of Appeals for the Sixth Circuit.

Michael earned a Bachelor of Science degree in Economics from Hillsdale College and his Juris Doctorate from the George Mason University School of Law. He is Life and Health Insurance licensed. He is a member of the State Bar of Michigan.