November 18, 2019

FOR IMMEDIATE RELEASE

Contact: Daniel J. Forte
617-523-7595
dforte@massbankers.org

HOW TO AVOID PHISHING AND HOLIDAY SCAMS

BOSTON, November 18, 2019 – While it's everyone's job to ensure cyber security at work, it's also important that consumers are aware of safe online practices at home. The Massachusetts Bankers Association offers a few tips to avoid holiday scams and other potential computer pitfalls.

Avoid Phishing Scams

Criminals have gone "phishing," and consumers are prime targets. Phishing is the act of sending pretext emails to unsuspecting recipients who may think it is an email from their own bank or credit card company. These emails usually reference problems with an account or some situation requiring a fast response from the consumer. While most phishing schemes send the emails randomly, sending thousands increases the likelihood that the scammers will reach some consumers who do business with that particular institution. The email or its links will use the institution's logo and other graphics to give the impression that it is actually the organization sending the email, or "spoofing" it. Most often, the communication will include a request to "verify" social security, account numbers, or passwords. **Don't do it -- your bank or financial institution will never ask for this information in an email.**

A variation of this practice attaches "spyware" to your computer which can record keystrokes and other activity. "Spyware" can gain access to your computer when someone opens and downloads attachments from odd or unknown emails. Phishers are also still using social engineering tactics through the telephone to collect sensitive information from would-be targets. In fact, robocalls and targeted phishing calls from obscure locations have seen a rebound the last several years. Our advice is don't answer or hang up and then block the number.

Monitoring for Suspicious Responses to an Internet Ad

With more and more consumers selling used items online through various marketplace sites, we advise you to be on the lookout for warning signs in your online interactions with potential buyers. In some cases, fraudsters will complain about an inability to meet to exchange goods or they'll cite a complication over shipping costs or currency exchanges. Beware of these warning signs. Money in these types of transactions should only be moving in one direction – to you, the seller. If you're selling a lot of items online, it's important to check with your bank that payments have fully settled and the funds are available in your account. If you deposit a check from a buyer, the item "clearing" is not enough – the bank must be confident that the item is fully settled and there is no risk that the check will be returned.

Avoid Email Scams

We've all received emails asking for cooperation in moving a large sum of money out of another country — and likely discarded these letters as scams. But fraudsters have become more sophisticated, and now send emails or documents bearing seemingly official seals and signatures. You might see a full title, department and address along with other information that a scammer would normally not be able to provide. The scammers pose as bankers, chief auditors, chief security officers, remittance officials, and directors of finance, directors of government or bank contract award divisions — all stating they have access to unclaimed funds, generally in inactive or delinquent accounts, with millions waiting to be claimed. Don't give them anything – they're all fraudsters. While it may seem harmless at first, such as asking for your fax or cell number, later, someone will ask for your social security or bank account number and money

will be wired out of your account.

Be Wary of Prizes, Trips, Lottery Winnings

These can come to you via email, the US Postal Service or over the telephone. There are numerous variations but, again, what they have in common is a request for you to advance funds to receive your prize. The scammers claim you have won the a foreign lottery, a trip or some other windfall and all you have to do is advance a "handling" fee to the sponsor or provide your bank account number. **Don't do it – no legitimate contest requires the winner to advance funds to collect a prize.**

Avoiding Computer Viruses and Understanding the Risks of Auto-Fill

Computer viruses make their way onto our computers by malicious software installing itself – most often by clicking improper links or downloading suspicious files. Never download ".exe" files attached to emails from unknown senders. Don't ever click through suspicious emails in your junk folders and verify that there are no emails from known senders before cleaning out the junk folder often.

One of the more unfortunate developments of recent years has been the increased security risk of the Autofill function that is standard on most Internet browsers and smartphones. Your computer doesn't even need to be compromised by a virus to be susceptible to Autofill security risks. Instead, it is possible for website developers to create invisible fields in the forms on their websites that trick your computer's Autofill function into inserting protected information such as username, password, home address or anything else that you have saved with the Autofill feature. While Autofill may save a few minutes, turning off your browser's password and Autofill settings is a good idea in this environment of "big data" mining.

Be Careful with Credit and Job Applications

Online job postings and applications can make it easier to find a new job, but criminals may create fake job postings that ask you for your social security number or bank account information. Never provide this information unless you have established contact by phone, or mail, or in-person with the company and verified that they are legitimate. Remember, unless you have initiated a call or contact, providing personal or financial information over the phone or Internet is never a good idea!

The Massachusetts Bankers Association represents approximately 140 commercial, savings and co-operative banks and savings and loan associations with 72,000 employees located in Massachusetts and elsewhere in New England.

# # #

Massachusetts Bankers Association, Inc.
One Washington Mall, 8th Floor
Boston, MA 02108-2603
Tel: 617-523-7595 / Fax: 617-523-6373
http://www.massbankers.org
Twitter: @MaBankersAssoc
Facebook.com/MassBankers