November 06, 2018

FOR IMMEDIATE RELEASE

CONTACT: Daniel J. Forte
dforte@massbankers.org
617-502-3888

HOW TO AVOID PHISHING AND OTHER SCAMS

BOSTON, November 6, 2018 – 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 scams and other potential computer pitfalls.

Avoid Phishing Scams

Criminals have gone "phishing," and consumers are prime targets. This 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 referencing problems with an account or some situation requiring a fast response. The emails are random, but sending thousands increases the likelihood that the scammers will reach some consumers who, indeed, 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. The communication will then include a request to "verify" social security, account numbers, or passwords. Don't do it. Your bank or credit card company knows this information and does not need to ask you for it. This is a fraudster. A variation of this practice attaches "spyware" to your computer which can record keystrokes and other activity. It can start by your opening attachments to odd emails, even those that look like they may have come from your friends. Or someone can call you on the phone and ask these questions. Hang up, unless you initiated the call.

Avoid Suspicious Responses to Your Ad on the Internet

This scheme often involves a legitimate ad that you place on the Internet in various websites or in social media, perhaps trying to sell a car, electronics or any pricey item. Someone responds and cites complications with currency exchange or shipping costs, and sends you a check for more than the selling price of your stereo or car or whatever you are selling. After depositing the cashier's check, you are then instructed to keep a portion of the extra money and wire or send a check for what's left of the overpayment to the buyer's agent/shipper. After you wire the money out of your account you may find that the check you received and deposited was counterfeit. An important rule: If you're selling something, funds should be moving only in one direction – to you. And make sure, after depositing a check and before you release the goods, that your bank has the funds. Don't simply ask if the check has cleared (there's no such thing), verify that the funds are in your account by asking "Have the funds been 'finally collected?'" A better rule of thumb: If a deal sounds too good to be true, it probably is. Another warning: A similar fraud using a counterfeit cashier's check can also occur after an online auction.

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 the letters as scams. But other fraudulent letter writers have become more sophisticated, without errors, and with 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 inactive or delinquent accounts, with millions waiting to be claimed. Others say they are kin to family members who died natural but unexpected deaths, or their relatives were killed in assassinations, military coups, or plane crashes, also leaving a tidy sum for the taking. Of course, you're thinking, No one would fall for that – sending money to cover transport fees or personal information to claim a "fortune" – until

someone does. You are still likely to see grammatically incorrect letters with misspellings and wild schemes; those are easy to spot as fakes. Then there are the good letter-writers – and they're all fraudsters. Don't give them anything. If it seems 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 rather than the massive influx you were expecting.

Be Wary of Prizes, Trips, Lottery Winnings

This bogus communication can come to you via email, the U.S. 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 Canadian or some other lottery, you have won 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.

Avoid Computer Viruses

Of all Internet frauds, this one is perhaps the most insidious. You receive an email with a tender header, perhaps with an attachment titled "I love you," or "call me," or just about anything that piques your curiosity. When you open the email, it attaches a virus inside your computer that records keystrokes, log-in names and passwords. And it does so without your knowing it. After you have visited 20 or 30 online banking or financial Web sites, it emails that information back to the criminal sponsor. Best advice: Don't open strange emails, especially those with an .exe file.

Be Careful with Credit and Job Applications

If you see a credit offer or a job posting online, you can complete an application or send in a resume. However, don't respond if it asks you for your social security number or bank account information. These can be provided later after you have established contact by phone, or mail, or in-person with the companies and have verified that they are legitimate. Otherwise, you could be providing personal information that could result in the draining of your bank account or the stealing of your identity.

Remember, unless you have initiated a call or contact, providing personal or financial information over the phone or Internet is not a good idea!

The Massachusetts Bankers Association represents approximately 150 commercial, savings and co-operative banks and savings and loan associations with 69,000 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