Protect Your Workplace's Online Security - especially during a crisis

COVID-19 is temporarily forcing many people to work remotely, often using home computers. Scammers take advantage of these situations and we are hearing reports of new phishing and fraud scams. Most scams can be avoided through continued vigilance and by following existing approval procedures. However, this remote work environment creates challenges that make both companies and individuals especially vulnerable.

Recently, fraudulent websites have popped up offering ongoing counts of Coronavirus cases or other Covid-19 related information. Some of these sites install malware onto your computer or mobile device to track keystrokes, steal passwords, etc. Sticking to known news outlets is one way to minimize this new threat. Clicking links in Facebook, Twitter or even links sent by friends or found inside other news stories greatly increases your risk of becoming a victim.

Scammers use these crisis events to increase phishing scams that attempt to trick you into providing Payment Card information, Social Security Numbers, account passwords or other information they can use to hack an account or steal your identity.

- Never respond to (or click links within) emails that claim that an account has been compromised, your payment was rejected, your mailbox will be terminated, or anything similar. This is exactly how scammers phish for information.
- If your credit card account is compromised, you might receive an email, but it will direct you to call the customer service number on your card.
- If your mailbox is getting full, you might get an email alerting you, but it will not ask you to click on a link and login.
- No email or other system will ever contact you saying that your account will be terminated if you do not click a link to confirm you still want it. They might remind you that your account exists but they will ask for your password.

Even if an email looks completely fine, if you are asked for personal information, account information, passwords or other private data, verification that you still exist or anything similar, it is very likely a scam. Call the provider if you think it might be real or open the website directly in your browser to contact them (not by clicking a link or cutting and pasting).

As always, if you receive an email asking you to do something outside normal business practices like opening a file that you were not expecting or anything that feels new or wrong, always err on the side of caution.

- Call the sender directly to confirm, especially when money, account access, link clicking, or file downloading is involved.
- Do not reply to the email as it may have come from the hacker.
- Do not call the person using a phone number in the email as it may be the number of the hacker.
- Do not send a new email back to the sender as the sender's email account may have been compromised in which case you will be corresponding with the hacker.

Every business should have standard processes in place to avoid these sorts of scams.

- If you are instructed to wire money to a new location for a vendor, confirm it using normal accounting procedures.

- If you are asked to change someone's direct deposit information, follow the standard processes to get a signed request and confirmation with the employee.
- Do not let this remote work environment lull you into cutting corners and "taking care of the paperwork" later.

One new challenge that we all face is the increased use of Microsoft O365, DropBox, and other cloud services for file sharing. If you receive an email telling you that someone has shared a file with you and you must click a link to access or download it, be wary; the challenge is that some of these emails are legitimate. Some of us use external providers to send encrypted messages that require you to set up an account or login. All these realities open the door for scammers to trick you into clicking a bad link. The best way to avoid this is through communication. Again, call the sender to confirm a request of file transfer is real. If you are sending a file this way, especially to a large group, consider pre-emptively sending an email to the recipient(s) telling them that you are going to send them a file or encrypted link, especially if the recipient is not someone that is familiar with you or the tools you use.

Also, please do not forward suspected scams to IT asking for an opinion. Call the requester directly if you think a request or directive might be real. If you must get an opinion from IT, please use Snipping Tool or some other method to take a snapshot of your screen; even your phone's camera will work. Send the snapshot rather than forwarding the email. Oftentimes IT's own antivirus software will block forwarded scams or, worse, you will inadvertently compromise the IT person's computer as well.

Lastly, with regard to working remotely, if you are using a home computer for work and the home computer does not have functioning antivirus software, it is critical that you install an antivirus program and ensure that it is updating itself regularly. You should do this for your own safety anyway as your personal security is at risk without effective antivirus software in place. That fact that you are using the home computer to perform company work only exacerbates the risk. Also please remember that you should regularly backup your work. If whatever equipment you are using is not directly connected to the office network or cloud environment ensuring that your work is backed up and secure, please at least copy your files to a flash drive every day and remove the flash drive from the computer. Ideally rotate two flash drives in case one fails while you are backing up. With all of us struggling to work efficiently, we certainly do not want to compound the problem by losing work due to an equipment failure or virus attack.

Here are a few examples of scams we have seen. This list is by no means exhaustive. Remember, your vigilance is our first line of defence against these and all other scams.

- Attempts to get the payroll department to change direct deposit information for an employee
- Emails from people claiming to have recorded embarrassing internet activity which they threaten to send to your contacts if you don't pay them
- Offers of free services like Amazon Prime if you just click a link and log-in with your account info
- Emails impersonating people in the company attempting to get you to wire money or send gifts to clients
- Fake invoices that appear to come from real companies that you do business with trying to get you to pay for things never actually ordered
- Warnings that an account password was compromised that then asks you to enter your login ID, old password and a new password
- Warnings that your email box is full then asking you to enter your password to increase the mailbox size

The bottom line is these very dangerous scams and fraud attempts are typically recognizable and preventable if you stop and ask yourself if something seems wrong or unusual. If it does, follow up your suspicion with a phone call. For both your personal safety and the safety of the company, please continue to be hyper-vigilant, suspicious of all email requests, and practice safe computing, now and at all times.