April 2020

Arnett Carbis Toothman LLP
CPAs & Advisors

actcpas.com

COVID-19 Solutions for Work also Introduce Security Risks

COVID-19 has changed almost everything in our daily lives. One of those items has been an increase in the number of employees working from home. Technology has allowed working remotely for several years, but while the ability to work from home has provided many employees the opportunity to stay productive, the mass transition of people working remotely also magnifies the opportunity for fraudsters to take advantage of the current situation. Why? The fraudsters realize that more files are being moved through email and file transfer services. They also realize that many, if not most, of the IT security at Company personnel homes is not at the same level as working from the office.

COVID-19 is fluid, with changes happening on a continual basis. There are many programs and changes resulting from laws and regulations. Those changes include relief from the IRS regarding filing deadlines and tax payments, stimulus payments, CARES Act and others. With all of these changes, there have already been incidences of fraudsters attempting to take advantage and obtain nonpublic information as they masquerade as legitimate organizations.

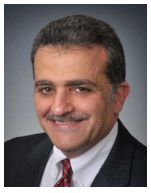
How do the fraudsters attempt to take advantage?

- Sending fake emails in an attempt to get the recipient to click on a fake link allowing access to the recipient's computer and releasing malware. Emails have been sent regarding basic supplies such as paper towels and toilet paper. In some cases the fraudster has sent emails confirming fake orders where they attempt to have the email recipient click on a link that could activate malicious software or they attempt to obtain nonpublic information from the recipient.
- Releasing malware through email attachments.
- Compromising another computer that may have company employees listed in their email address book. After obtaining the address book, fraudulent emails are sent to the addressees masquerading as the person that had company employee contact information.
- Infecting computers with ransomware.
- Taking advantage of security weaknesses that exist to address children's educational needs. In some areas, school children have experienced challenges with obtaining and completing their assignments. Schools have attempted to provide additional access through drive-up internet wireless access located at the school. Unfortunately, the connections are not secured and could lead to unauthorized access, malware, etc.
- Taking advantage of unpatched systems.

What can a company do to enhance protection and reduce the risk of being exploited?

- Send reminder email communication to all personnel reminding them of the company's security policies – ongoing education is one of the best defenses.
- Educate users about the latest phishing attacks including issuing alerts of emails received by employees.
- Patch every system on a regular basis and critical issues as quickly as possible.
- Keep anti-malware solutions current and conduct regular scans.
- Backup all data on a regular basis to assist in the recovery process, if needed.
- Utilize secure remote access solutions and lock down remote touch points (i.e. RDP).
- Utilization of difficult to crack passwords including for service accounts.
- Where possible, utilize multifactor authentication.
- Emphasize to all personnel, when in doubt, do not click on the attachments, links or even open the email (i.e. continue to follow security policy). Forward all suspicious emails to the IT group for further review and consideration.
- Do not use company resources to login to unsecured access points.
- Educate, Educate, Educate

While we are all trying to come together to fight COVID-19, unfortunately many fraudsters and cybercriminals will not hesitate to exploit security flaws. Ensure company personnel follows security policy, educate all personnel and remain fluid in the company's security posture in this time of constant change and challenges.



Christopher Joseph, CPA, CISA, CRISC, CITP
Consulting Services | Partner
chris.joseph@actcpas.com
304.346.0441 | 800.642.3601