CPA
Practice Advisor

their affairs in order to meet the extended deadline.

Mar. 25, 2020

Because of the COVID-19 outbreak, the government has extended the deadline for filing 2019's taxes to July 15. But they suggest firms and individuals with a potential tax return to file asap to get access to these funds.

In the next few weeks, many firms struggling during the recession will rush to file to get their returns. Others may use this time as a needed reprieve to start getting their affairs in order to meet the extended deadline.

Between this and the vast number of workers who've shifted to telecommuting, the amount of vulnerable corporate data has skyrocketed. And cybercriminals are well aware of this. They have ramped up their number of attacks on both business

and steal employee identities. That's why, every year, tax season is one of the most active times for cybercrime.

Even with the extended deadline, this year is no exception. In fact, because of the COVID-19 outbreak, hackers are more active than ever.

Problem 2: Remote Isn't as Secure

Most business networks have some form of enhanced network security. Many use firewalls, VPNs, anti-malware, and other tools. They create comprehensive protection against cyber threats. Employees' home networks and personal devices are usually no match for corporate ones.

But many workers now work remotely. So they're much easier targets for hackers. Most home networks contain few if any security protocols. And, if they do connect to secure networks, the connections themselves may not be secure.

Hackers can deploy man-in-the-middle attacks and malware to intercept data-in-transit. Not only does it include tax records but also other data sent between corporate networks and unsecured devices.

Problem 3: Confusion is Everywhere

The story changes every day. Authority only recently delayed taxes. What if they do that again? Do individuals still need files? Are there any new deductions for businesses in the wake of this concept? It's enough to make your head spin.

Taxes are difficult enough to do in an average year. This year has created mass confusion, which hackers consider a golden opportunity to exploit. For example, they've started sending social engineering emails related to the current events. "Immediate Response Required Due to COVID-19" is one such example.

These emails are a far cry from Nigerian Prince Scams. They take unsuspecting

Whether for personal or your business, it’s essential to review how to file taxes. If you or your employees have individual tax refunds waiting, this is the time to apply for them to get some relief.

If you haven’t filed corporate taxes already, take the time to see what your company owes. The federal government and most states may have tax credits or other forms of help available.

You can’t predict what will happen over the next few weeks and months. But you can prevent cyber-attacks from affecting your business and personal networks.

Hackers don’t want tax documents only. They’re interested in corporate data, files, media, contact and customer information, and other vital data. And it’s all on your business or personal devices. Be sure to instruct all employees to follow digital security practices, such as:

- Securing all online accounts with unique, robust passwords
- Using two-factor authentication and other account security tools
- Protecting all network connections with a virtual private network and firewall
- Locking all devices with passcodes and other tools
- Recognizing suspicious emails and websites
- Using antivirus and antimalware software
- Scanning all files and links before opening
- Encrypting all data on local and cloud storage drives

- Encrypting all files at rest and in transit

interest is cybersecurity and the main goal is to raise awareness around the threats that people and businesses can face online.

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.