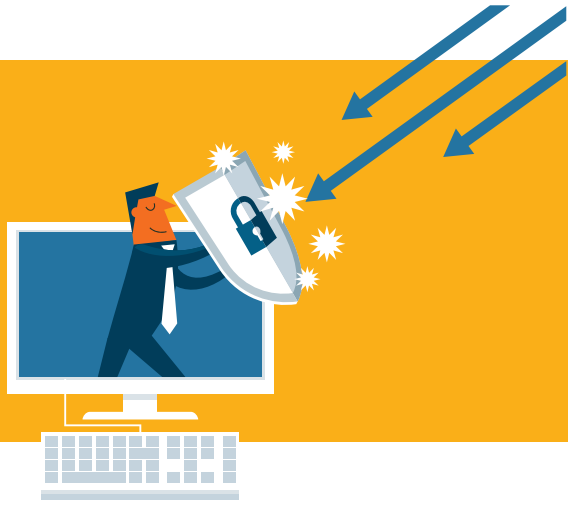
Cybersecurity in a post-pandemic world



The Coronavirus crisis has changed the world as we know it. With social distancing, lockdowns and work from home becoming the new normal, cyber criminals are exploiting the situation. This whitepaper discusses how the cyber crime landscape is likely to shape up in the post-pandemic world and how businesses can safeguard themselves against it.

One of the reasons for a sudden spike in cyber crime is the work-from-home model that is increasingly becoming the norm. When you allow remote access to your data, you are virtually opening your IT infrastructure to criminals--unless you have the right security measures. It is easy for malware and hackers to get into your system and corrupt it unless you have the right measures in place. With employees operating from home, there are a lot of loopholes that cyber criminals target. Some of them include

Lack of knowledge

Most employees don't realize how their simple actions or non-actions can permit a cyberattack that can bring your whole business down.

It is more difficult to oversee IT operations

With teams working remotely, it is difficult for businesses to manage their IT efficiently. Installation of security patches, anti-malware tools, data backups, etc., are all more difficult now.

What can you do to ensure your business is not a victim of cyber crime during work-from-home?

Does that mean your work-from-home model is not viable? Not really. A lot of companies, in fact, are contemplating a permanent work-from-home model even after the Coronavirus situation ends, as the benefits of the model are now clear to them--it offers a lot of flexibility and helps save on overhead costs.

You can still have a remote workforce while keeping your data safe. There are just a few things to consider.

Formulate rules

You can start by formulating rules that define the extent and manner in which personal devices may be used for work purposes.

- Who is allowed to use personal devices for work?
- Spell out the regulations that they must follow. For example, regular checks for malware and updates to anti-malware software, etc.,
- If there are restrictions to the device type, software or operating systems that may be used, out of security concerns, then these should be addressed.

Focus on the 2 Ts of cybersecurity

- **T**rain your staff: The first T is training your staff on how to identify IT threats and cybercrime activities that they can be a victim of. Examples include phishing emails, dubious attachments, clone sites, etc., Another area to train your staff about is the use of free/public wifi. They need to know that public wifi can be a gateway for hackers and cybercriminals into your system. Accessing emails from the airport's waiting lounge or the mall's food court can expose your business to IT threats.
- **T**each good password hygiene: This is the second T. Help your employees understand how important password strength is. They should be able to identify weak passwords and steer clear of them. Also, they need to know that no matter how urgent the situation seems, password sharing is not acceptable. Similarly, mistakes such as repeating the password for multiple accounts, not changing the passwords frequently, etc., can make a cyber criminal's job easier.

Keeping things under control

You can conduct monthly audits of the devices your employees will be using for work purposes. Arrange for regular security patch implementation, firewall installation and software updates. Install quality anti-malware software, firewalls and email security systems. Even in the remote environment, you can ensure appropriate data access through role- and permission-based access control measures.

With a strong IT policy that caters to the work-from-home environment, you can make this new normal work for you. However, it is important to clearly define the policies and actually put them into practice. All of this may seem new, and tedious, especially for businesses that are looking to recover from the effects of the on-going pandemic, which is why it is a good idea to team up a managed services provider to help set up a strong, secure, work-from-home environment for your business.

For more information please contact,
Madinah Ali | President | SafePC Solutions
Phone: 1-404-631-6620 | Email: msali@safepcsolutionsusa.com

SAFE PC® SOLUTIONS

1100 Peachtree Street, Suite 200 NE, Atlanta, Georgia, 30309
http://www.safepcsolutionsusa.com