Driving Office Productivity through Managed Print, Document Solutions, Enterprise VoIP Systems, and Managed IT Services

LANG

www.langcompany.com

A Prescription for Cybersecurity

Lose weight, exercise more, eat your vegetables, and get your annual physical. Simple, proactive measures that prevent illness and uncover issues before they become major problems. The same approach should be used when it comes to cybersecurity.

Being proactive and adopting healthy practices around your technology infrastructure is the most effective way you can prevent an attack or limit the damage should one happen. Experts often cite that 60% of business that suffer from a ransomware attack will close within 6 months. Follow these steps to improve your chances of being in the minority who survive.

Creating Healthy IT Habits

If some of these seem obvious, they are. Unfortunately, we still see some organizations neglecting to do even the most basic levels of cyber security. Here is the list:

Passwords: Should be required on ***every*** device that logs into your network, including phones. They should contain at least 8 characters and use a mixture of upper- and lower-case letters, numbers, and symbols. You should require password changes every 3 months at a minimum.

a. Example of a bad password: Password21
b. Example of a good password: %Tve@l0Bx!

If you have trouble keeping track of your passwords, use a Password Manager program to help you. If you are serious about security, you should be using multi-factor authentication (MFA) to log into critical programs or infrastructure, including email.

Anti-virus and Malware Software: It should be installed, enabled, and set to update automatically. Free AV software is better than nothing, but the old saying of "you get what you pay for" is a wise old saying for a reason.

Security Updates: Those annoying, "please do not shut down your computer" notices contain valuable security patches. Set them to automatically download and install. Restart your computer as soon as the update is available. If your computer is too old to receive any updates, upgrade it at once. It is highly vulnerable to an attack.

Firewall: You should have a firewall. Most likely you do, but is it doing the job? Firewalls come in many different varieties. There are major differences in how effective they are at stopping intruders from entering your network. If your firewall is older or you purchased it because it was cheaper than the others, you are probably at risk.

End User Training: Most security breaches are still caused by human error. Falling for a phishing scheme or clicking on a bad link is the cause for most successful hacks. Making sure your users are trained to identify and avoid these traps is key to your cyber defense. Following up with testing to see who in your organization needs additional training is a smart move as well.

Routine Maintenance: Remove former users from Active Directory and old devices from the network. These pose a significant security risk. It is not uncommon for us to find former employees with active log-in credentials or devices on the network that no one uses. It is usually an oversight of some kind that opens the gateway to your network.

DNS Filtering: DNS filtering protects by blocking access to compromised websites, spam-based websites, and malicious websites. It also can free up network resources and bandwidth by giving you the ability to block visits to sites like Spotify, YouTube, & ESPN among others.

Proper Data Back-Up: Best practices say you should back up your data both locally and in the cloud. There should be multiple versions in case one gets infected or locked. Also, make sure you test your backup recovery at least once per quarter. Finding out your back-up is useless when it's the only thing keeping you in business is worse than not having a back-up at all.

Segregation of networks: Don't put all your eggs (or data) in one basket. With so many devices capable of logging onto your network, it makes sense to keep them separated. Visitors, back office, and manufacturing should all have their own network. Visitors and vendors go on a restricted guest network while employees work within the business network.

Advanced Security Tools: This suite of products and services combine advanced security tools using artificial intelligence, machine learning, analytics, and a staff of security experts to predict, identify, and prevent attacks that typical virus protection would miss. It will also analyze end user and network data patterns to spot suspicious changes in activity to identify and halt the attack and damage before it can spread.

Dark Web Scanning: The Dark Web is where all that stolen data goes on the market. Passwords, emails, personal information, and more is up for sale. By continuously monitoring the Dark Web for personal information, you can take action to protect yourself before criminals can gain access to your data or steal your identity.

Encryption: Having your files encrypted in a ransom attack is bad. Using encryption to prevent others from gaining access to the data on your files is good! You can employ different levels of encryption from data at rest to end-to-end encryption. Choosing the right level for you depends on many factors that are unique to your organization.

Cyber Insurance: When all else fails, cyber insurance will help offset the costs associated with a ransomware attack. Don't assume that your general liability insurance will cover these claims. It usually does not. There are several types of protection available. It is best to consult with your Cyber Insurance professional to make sure you are covered.

These are some of the ways you can protect your organization from being a victim of a cyber-attack. How did you do?

Hopefully, you are already utilizing many of these security measures. But remember, your best defense is only as good as your weakest link. Keeping criminals out 99% of the time is statistically great, but it only takes one opening to bring your business to a halt.

Time for a Check-Up?

If you would like an assessment to see where your cyber defense may be weak, we offer a security assessment that will provide detailed feedback on where you may be vulnerable. For more information, please call 888-700-0237, or visit https://langcompany.com/managed-it-services/network-assessment/

IT365 is a division of Lang Company dedicated to helping companies leverage their IT infrastructure to help them succeed in business. We use a proactive, comprehensive approach to give you a reliable, predictable, and secure technology platform so you can focus on your business.

IT365…Always on and working for you!