"Top 20" Must-Haves for Cyber Protection - The Best List!

There is no single product available that will solve all of your cybersecurity problems. In today's world, you need a "layered approach" to keep the bad guys out. Here are the top 20 ways to help significantly reduce your risk!

1 Keep your operating systems updated

Make sure your all your computer, smartphones and tablets are set for auto updates – and be sure to re-boot when you get the notifications.

Anti-virus and anti-spam 2

A basic 'must-have' - but stay away from free or consumer products and consider an automated process to ensure you're always up-to-date with the latest.

3 Strong password policy

Your IT policy (you have one, right?)should include mandating complex passwords, and network settings should require employees to change passwords frequently.

Use Auto Screen lock

4

When a PC or mobile device has been idle for a few minutes, it should be set to automatically lock the screen. Seems simple but many neglect to do this.

Document where all your data resides, including servers, workstations, mobile devices, thumb drives, backup systems and cloud locations – and limit who has access.

Locate Your Data 5

Physical Security 6

On-premise file servers need to be in a locked room/cage, the office should have a security system and mobile devices need to be locked when not in use.

When implementing firewalls and security-related features such as remote access and wireless routers, make sure they're properly configured, up-to-date and receive regular patches.

Firewalls and Routers 7

8 Minimize Administrator Privileges

Don't let workstations run in administrator mode – this exposes them to more security threats and can lead to the entire network being infected.

This is a must for any business that must remain PHI or PII compliant.

9 Email Encryption

Choose a standardized tool that allows for the secure sending and receiving of sensitive files and make sure staff are educated on using encrypted email for confidential data.

Train staff on how to connect securely to company data when not in the office, via VPN or other secure connection - and remind staff never do any confidential work on public WiFi.

10 Connect Securely

11 Protect Mobile Gear

While laptops have often been cited as the top mobile theft risk, mandatory passwords and data encryption should be extended to smartphones and tablets.

Be sure you have IT policies that provide guidelines and rules for computer and Internet usage, BYOD, Remote Access, Privacy and Encryption.

12 Create IT Policies

13 Educate Employees

In addition to training on IT policies, employees should be educated on current cyber security attack methods such as phishing and ransomware – consider using simulation tools that test employees on a regular basis.

Firms should do a thorough background check on all potential employees or contractors before allowing them access to valuable resources.

14 Screen Potential Employees/ Contractors

Despite your best efforts, the chance of a data breach in today's world is extremely high. Be sure you have the best BDR solution in place – do not rely on outdated technologies you've had in place for years!

Backup and Data Recovery (BDR) 15

Encrypt Backup Data 16

Encrypt any backup media that leaves the office and also validate that the backup is complete and usable, regularly review backup logs for completion and restore files randomly to ensure they will actually work when needed.

Different from BDR, a business continuity program documents how your organization will respond to, continue through and provide normal levels of service despite severe disruptions.

17 Business Continuity Program

Many firms must have a Business Continuity Program to meet industry regulations.

18 Breach Response Plan

Have a formal security incident response plan in place in the event that there is concern that your data has been compromised, including an internal and external communications plan.

Cybersecurity Insurance 19

Unfortunately, firms can do all the right things in regards to security and still fall victim to a hacker - you may want to consider cybersecurity insurance which is not as expensive as it used to be.

Every organization needs to perform an annual audit as the cyber security landscape is constantly changing – and in some cases, your business may be required to have an external auditor certify your compliance.

20 Security Audit

Sound like too much to deal with on your own?

It pays to hire outside expertise when your most precious company asset – your data – is at risk.

Ntiva can help.
Contact us for a Complimentary Security Consultation.

info@ntiva.com | 703-214-9540 | www.ntiva.com