8 Urgent Security Protections You Should Have In Place Now

Cybercrime is at an all-time high, and hackers are setting their sights on "low hanging fruit." Don't be their next victim! This report will get you started in protecting everything you've worked so hard to build.

The average ransomware payment in 2021 was reported as $118,000.
A total of 1,962 data compromises were reported by US organizations in 2021.
COVID-19 scams are still popular with attackers. The latest variant has led to a 521% increase in attacks.

39% of businesses say they lack internal expertise to develop a zero-trust model and increased security protections.
Where do you stand?

Provided By:
Asset Technology Group
213 S. Main St
Darlington, SC 29532
843-868-3002
www.assettg.com

Businesses who suffered data breaches without security protections in place could have saved millions of dollars with Security Automations, having an Incident Response Team, performing Employee Network Security Education and Performing Regular Tests. This report aims to help you implement proactive management of your networks to keep you from becoming just another statistic.

As bad actors are increasing the intensity of attacks, ranging from attacks on vulnerable systems to well-crafted phishing campaigns, there are security measures you can put in place TODAY to prepare for a safe and secure TOMORROW.

1. **<u>Train employees on security best practices.</u>** The #1 vulnerability for business networks is the employees using them. It's extremely common for an employee to infect an entire network by clicking bad links or downloading malicious content from a phishing email. If they do not know how to spot infected emails or online scams, they could compromise your entire network. Hackers are betting on you being too busy or so intrigued by an offer in an email, that you take the bait and fall victim to a phishing attack.

ASK US ABOUT ONLINE SECURITY TRAINING AND PHISHING EMAILS DESIGNED TO EDUCATE, TEST AND HELP PREPARE YOUR STAFF FOR POTENTIAL ATTACKS !!

2. **<u>Implement a Zero-Trust model.</u>** Zero trust is a security model based on the principle of maintaining strict access controls and by not trusting anyone or any action by default. Each transaction (updating software, installing new applications, etc.) is evaluated for need and risk. In a networked world full of threat actors - Never trust. Always verify. We apply a zero-trust architecture for our clients, as an extra layer of threat protection. As attackers become more sophisticated, so must your endpoint protections. Helping to block potential malicious programs, ransomware and malware, this model effectively protects your organization against evolving cyber threats.

ASK US ABOUT T-SHIELD. OUR BEST-IN-CLASS SECURITY PROTECTIONS PLATFORM. PROTECT YOUR ENVIRONMENT FROM INTERNAL & EXTERNAL THREATS.

3. **<u>Require STRONG, COMPLEX passwords for all network-connected devices and mobile devices.</u>** Passwords should be at least 8 characters and contain lower and uppercase letters, symbols and numbers. Strong passwords to access network-connected devices (computers, etc) can be ENFORCED by your network administrator so employees do not get lazy and choose easy-to-guess and easy-to-crack passwords. Multi-factor-authentication can also be enforced as well as regular password updates. Proper management of passwords is also important – secure password managers can be installed, helping to keep all passwords safe instead of stored on a browser or on a sticky note for the world to see.

WANT SUGGESTIONS FOR THE BEST PASSWORD MANAGERS? DOES YOUR STAFF REUSE PASSWORDS AND SHARE THEM? GET BETTER PROTECTION TODAY & ENFORCE BETTER PRACTICES.

4. **<u>Keep your network up-to-date.</u>** New vulnerabilities to common programs you are using, such as Microsoft and even browsers, are in the news every day. It is critical to patch and update systems frequently to ward off potential attacks.

ATTACKERS CAN SEEK OUT THE VULNERABLE MACHINES. DO NOT FALL VICTIM TO COMPROMISE FOR LACK OF PRO-ACTIVE MAINTENANCE AND REGULAR SYSTEM UPDATES.

5. **<u>Don't skimp on a good Firewall.</u>** A firewall acts as the frontline defense against hackers performing malicious attacks on your network. A well-configured firewall is crucial to protecting your organization. Monitoring and maintenance is also required, just like with maintenance to devices. This should be done by your IT person, as part of their regular, routine maintenance.

DOES YOUR IT PERSONNEL STAY IN THE KNOW WITH THE LATEST HACKING TOOLS? ARE THEY PREPARING YOUR NETWORK WITH THE BEST DEFENSES?

6. **Have an excellent backup solution.** This can foil the most aggressive ransomware attacks, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up in a secure off-site location, you can be back up and running quicker than you think. A good backup will also protect you against an employee accidentally (or intentionally) deleting or overwriting files, natural disasters, fire, water damage or hardware failures. Backups should be automated, monitored and tested frequently to ensure it will work when you desperately need it most.

ARE YOU STILL RELYING ON VULNERABLE TAPE BACKUPS?
ADVANCE YOUR BACKUPS WITH A SECURE, OFF-SITE TOOL.

7. **Create an acceptable use policy-** and enforce it! An AUP outlines how employees are permitted to use company-owned PCs, devices, software, internet access and email. Limiting how employees are to use devices is crucial. Content-filtering software and firewall configurations should also be enforced, by setting up permissions and rules that regulate usage. Clearly outlining use of secure connections, how sensitive information is retrieved, used and stored, and policies for using personal devices can help ward off attackers.

IF AN EMPLOYEE LEAVES YOUR ORGANIZATION, DO YOU HAVE AN EXIT POLICY IN PLACE FOR DEACTIVATING USERS?

8. **Anti-virus!** Encryption technology to protect network data and anti-virus software to protect against viruses and other threats, are oh so important solutions to prevent sabotage and loss of data. Our anti-virus software is just one more layer of the onion of threat protections we offer to our clients. Anti-virus can protect your network when

employees visit bad sites, click those click-bait ads on browsers, and more. Without this very important element, you are at great risk.

AS YOU PEEL BACK THE LAYERS OF YOUR THREAT PROTECTIONS, IS ANTI-VIRUS ONE OF THE TOP DEFENSES?

Want help in implementing these 8 essentials?

We can customize a security solution to safeguard your network. Very simply, cybersecurity is like an onion. As you peel back the onion of threat protections, you uncover the many layers of protections that are necessary to safeguard a network. Encryption, anti-virus, tight firewall, zero trust, sandboxing – just a few layers to mention….

But the protections do not stop there. There is employee education, pro-active maintenance of devices, patches to critical updates of software and applications, multi-factor authentication…

I know it is natural to think, "We've got it covered."

Are you 100% confident in your cyber security platform?

Get the facts. Be certain your organization is implementing first-in-class security protections as we face ever-evolving threats.

Hackers only need to get it right once- We have to get it right every time.

For more information about our services or to set up an appointment for a network assessment to give insight into where your network stands, give us a call today. We welcome the opportunity.

Asset Technology Group
213 S. Main Street
Darlington, SC 29532
www.assettg.com
information@assettg.com
843-395-1467