7 Ways to Keep the Monsters Away Checklist

These seven items are necessary for companies in today's digital world:

Security Awareness Training - Protecting your business from ransomware starts by educating your staff. Around 90% of ransomware arrives via the inbox as a phishing email. Ensuring employees know what to do when one of these emails slips into their inbox is half the battle in keeping your company safe from this threat.

Firewall with Advanced Threat Detection – This is one of your business's first lines of defense. Everything from the internet must go through your firewall before it gets to your computers/network. A business-grade firewall will help keep the bad guys from slipping in. It would be even better to have a firewall with advanced threat detection. The difference is similar to a car with a backup camera and a car with a backup camera and beeping/too-close notification. The first one is good, the second one is best.

Antivirus Protection – Every device in your company that has access to the internet should have paid business-grade antivirus software. Free versions should be avoided since they do not update fast enough to protect against current threats. Your antivirus software should be set to completely scan files in real-time on all devices daily (at minimum).

Multi-factor Authentication - This is a cybersecurity measure for an account that requires anyone logging in to prove their identity multiple ways. This could be via text, an Auth App on your device, an email, or a phone call. Multi-factor authentication makes it more difficult for hackers to access your online accounts, even if they know your password.

Password Hygiene/Protection – No matter what the account, all passwords should be created with these three guidelines: long (at least 12 characters), unique (don't use the same password for your email and your banking), complex (use a combination of upper case, lower case, numbers, and special characters). Your business should have a strong password policy that discourages reuse and recycling of passwords and encourages using a password manager instead of sticky notes.

Dark Web Monitoring – Data breaches happen to everyone all the time. Don't wait until it's too late to find out that one of your employee's credentials has been compromised. In today's cybercrime environment, dark web monitoring is like the engine light in your vehicle. It will let you know that there's an issue and it needs attention. A paid dark web monitoring service scans the dark web data markets and hidden data dumps 24/7/365 for your company credentials and will notify you immediately if one pops up.

Zero Trust Policy & Access Management - Ensuring that only the right people have access to sensitive systems, databases, or financial information goes a long way towards preventing malicious insiders from stealing your data. There's no reason for the receptionist to have access to the accounting files unless they also handle the accounting. Limit access to only those who need it.

Bonus: Domain Protection – Protect your business brand by purchasing domain names similar to yours before hackers get to them. If they are available, you want to get the obvious spelling errors along with the .net, .co, and .info. All domain names purchased should be in the company owner/CEO's name. Ensure that you have full domain protection turned on to prevent unauthorized changes– this small extra cost per year could save some major headaches in the future.

GSG Computers, Inc.
615-826-0017