PRO OnCall TECHNOLOGIES®

ProOnCall.com

Whitepaper

Network Security Basics for Your Business

Arnold Palmer famously said, "Golf is deceptively simple and endlessly complicated." Consider the goal of the game — hit a ball into a hole. Simple, right? But to accomplish that goal, you have to take into account dozens of factors. Even if you play the same course every day, no two rounds will be alike.

The complexity of all those additional factors lead a lot of golfers to believe that strengthening their game means getting serious about these little details. But if you're looking to improve your game, you don't start with an analysis of sophisticated, pro-level techniques. You start with the basics, like mastering the fundamentals of your swing.

In that sense, golf is a lot like network security.

> "50% of all SMBs have experienced a cyberattack in the last 12 months."
>
> — SecurityIntelligence

Mastering the Basics

Network security is in the news a lot, and for good reason. Experts estimate that the global impact of cyber crime will cost more than $6 trillion by the year 2021. What's more, roughly 50% of all SMBs have experienced a cyberattack in the last 12 months. New threats emerge on a near-daily basis. It's a full-time job simply keeping up with current security trends.

A lot of SMB owners mistakenly think the key to protecting their organization is to delve into the nitty, gritty specifics of the latest cyber crime trends. But, like golf, the key to keeping your company safe lies in mastering the basics.

Cyber crime tactics are always changing, and they will continue to do so. However, the core components of network security are more or less stable. If you want to protect your data from cyber criminals, good places to start are:

"66% of [data protection leaders] admit that employees are the weakest link."

— Experian

Determine Your Network's Weaknesses

Knowledge is power. Using penetration tests to hack into your own network will help you understand where your business needs to bolster its security. Strengthening your network's weaknesses will help you avoid being hacked, maintain 24/7 business continuity and ensure that compliance standards are continually being met.

The more you are able to prepare, the more likely you are to prevent cyberattacks and data loss in the future. Additionally, getting into the habit of performing routine security audits will help you avoid becoming a cyber criminal's next victim.

Update Your Passwords Often

Frequently updating your company passwords is one of the easiest, most essential things you can do to protect yourself against being hacked. Cyber criminals are skilled in the art of password cracking. Passwords are based on patterns. If you frequently use the same password (or a similar variation) for your logins, hackers will be able to crack them all in a short amount of time.

In addition to changing them frequently, be sure to use a variety of characters, numbers, and letters when creating your passwords. The harder they are for you to remember, the harder they're going to be for an outsider to hack.

Encrypt Your Files

An excellent way to protect sensitive data is to encrypt it. When you encrypt your data, you're essentially scrambling it into undecipherable script that has no rhyme or reason. The key to read this data lies in login credentials that are set up specifically for those files. Those without those credentials will be out of luck. Thus, if your encrypted files happen to fall into the wrong hands they'll be protected.

Monitor Internal Activity

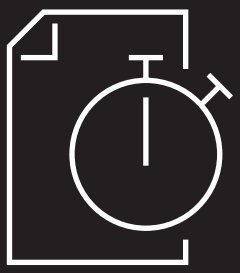
Experian noted that "66% of [data protection leaders] admit that employees are the weakest link" when it comes to maintaining a secure network. Often, they unknowingly put your network's security at risk.

Keeping an eye on the various sites your employees are visiting on company devices can help you prevent security breaches. If you see a member of your staff has visited a potentially dangerous site, add the page to your network's blocked list.

Keep Your Firewall On, Always

A firewall is a security system that, based on a set of predetermined rules, decides what data enters your network. Its main purpose is to protect your business from cyber criminals that want to gain access to your company's confidential information. It also prevents unsafe connections from unknown devices and hides your computer's IP address, making it extremely hard to find and compromise.

With "75.6% of organizations having encountered at least one successful cyberattack in the past 12 months," keeping your firewall on at all times is an excellent way to help prevent unwanted security breaches and data loss.



"98% of organizations say a single hour of downtime costs over $100,000."

— ITIC

Install Antivirus Software

The first tool in a strong network defense system is a solid antivirus program. This kind of software will do a daily scan of your systems and remove malware that has managed to make its way past your firewall. The best versions of these programs will update themselves daily, keeping current with new malicious software threats.

What are the Business Benefits of Network Security?

Network security helps protect customer data, employee data, proprietary information, and reduces the risk of legal action if that data is lost. While this is certainly a substantial benefit, perhaps the largest advantage organizations receive by having a sound security system is protection against business disruption.

ITIC's latest survey found that "98% of organizations say a single hour of downtime costs over $100,000." This could be a virus that has taken over a portion of your network or files, denial of service attacks meant to bring your entire network down, or simple spyware and adware that can significantly limit everyone's ability to get their job done.

When businesses experience downtime, it will cost them. The longer the downtime, the larger the cost.

Let's Secure Your Network Together

There's really no limit to what could happen to your data without a comprehensive network security strategy in place. Working with PRO Oncall to establish this plan will keep your organization running smoothly, your data confidential, and your company's reputation in good standing. If these sound like things you're interested in, contact us today. Let's bolster your business' security, together.

PRO OnCall TECHNOLOGIES®

Corporate Headquarters

12125 Ellington Court
Cincinnati, OH 45249
Phone: (513) 489-7660

Cleveland Office

5145 Brecksville Rd., Suite 205
Richfield, OH 44286
Phone: (440) 526-2500

Columbus Office

281 Cramer Creek
Dublin, OH 43017
Phone: (614) 761-1400

Dayton Office

733 Congress Park Drive
Dayton, OH 45459
Phone: (937) 294-5900

(800) 362-6300
ProOnCall.com