ISSUE 24 WINTER 2019

Newsletter

What's Inside

Cybercriminals Are Taking Aim At Your Business ... Is Your Network Protected?

Cybercriminals love to test your defenses. They love to see how far they can get into the networks of businesses all over the globe. Cybercriminals really love going after small businesses because they can all too often sneak onto a network, copy data and move on. Through the use of ransomware, they can hold your data hostage and refuse to cooperate until you pay them some amount of dollars – and if you don't pay up, they threaten to delete all your data.

But protecting yourself is not as hard as you might think. While cybercriminals and hackers are an everyday threat to businesses, you can take steps to significantly reduce that threat and take that target off your back.

The first thing you need to do is understand why cybercriminals target small businesses and what makes your particular business vulnerable. There are many things small businesses do and don't do that open them to attack and data theft. These may include not having enough (or any) security in place or not training employees on security protocols.

Realistically speaking, the biggest threat to your business does, in fact, come from your own employees. This doesn't mean they are intentionally harming your business or leaving your network exposed to outside threats. It means they don't have the proper training and knowledge to protect your business from a cyberthreat.

For instance, your team needs to be trained to use strong passwords, and those passwords must be changed periodically (every three months is a good rule of thumb). A lot of people push back on strong, complicated passwords or use the same password for everything, but this is just asking for trouble and should not be allowed at your company.

Once strong passwords are in place, enable two-factor authentication (2FA) on everything you possibly can, from network access to every account you and your employees use. This is an additional layer of security on top of standard password protection. This feature is generally tied to a mobile number or secondary e-mail, or it may be in the form of a PIN. For example, when 2FA is enabled, after you've put in your password, you will be prompted for your PIN for the associated account.

Another thing you must do to get that target off your back is to get anti-malware software installed. Every workstation or device should have some form of this protection. Not sure what to use? This is when working with a dedicated IT company can come in handy. They can help you get the right software that will meet your specific needs without slowing you down. They will install software that is compatible with your PCs and other networked equipment. Plus, they will make sure anti-malware software is working and is regularly updated.

On top of this, you want to have an active firewall in place. Every business should have its network protected by a firewall; like anti-malware software, firewall security comes with a number of different settings, and you can customize it to fit the needs of your network. Firewalls help keep attackers and malicious software off your network. When paired with a good anti-malware software, your layers of security are multiplied. The more layers, the better protected you are.

Finally, with all of this in place, your employees need to know what it all means. Keep your team up-to-date on your business's security protocols. This includes items like your password policy, malware protection policy and proper e-mail and web-surfing etiquette. The bad guys are never going to stop attacking, but you have the power to protect your business from those attacks.

5 Bad Business Security Practices

Companies — small- and medium-sized businesses, in particular — struggle to protect their data. For one, they make mistakes in the strategies they employ to protect their IT infrastructure. If your organization still does one or more of these bad security practices, act quickly to correct them.

1. Open wireless networks
With one main internet line and a couple of wireless routers, a whole office can go online. A wireless internet connection saves money, but there is an inherent risk that it's an unsecure network.

If you need a secure network, plugging in a wireless router and creating a basic network is not enough. If you don't set a password on your routers, then anyone within range can connect.

Therefore, you should take steps to ensure that all wireless networks in the office are secured with strong passwords. Many internet service providers that install hardware when setting up networks will often just use an easy password for the router, such as the company's main phone number. These need to be changed.

2. **Email is not secure**
Most companies that have implemented a new email system in the past couple of years will most likely be secure. This is especially true if they use cloud-based options or well-known email systems like Exchange, which offer enhanced security and scanning.

The businesses at risk are those using older systems like POP, or systems that don't encrypt passwords (what are known as "clear passwords"'). If your system doesn't encrypt information like this, anyone with the right tools and a bit of knowledge can capture login information and compromise your systems and data.

If you are using an older email system, it is advisable to upgrade to a newer one, especially if it doesn't use encryption.

3. **Mobile devices that aren't secure enough**
Mobile devices offer a great way to stay connected and productive while out of the office. However, if you use your tablet or phone to connect to office systems but don't have security measures in place, you compromise your networks.

Imagine you have linked your work email to your tablet but don't have a screen lock enabled, and you lose your device. Anyone who picks it up will have access to your email and all your sensitive information. The same goes if you install a mobile device app with malware on it. Your infected device will spread this malicious program to your entire network and cause major disruption to your business.

Lastly, mobile device management solutions are specifically designed to prevent your bring your own device (BYOD) policy from being a risk with employee devices causing havoc to your network.

4. **Anti-malware software that isn't maintained**
These days, it is essential that you have anti-malware software installed on all devices in your company, and that you take the time to configure these properly.

It could be that scans are scheduled during business hours. Updates are important for software, especially anti-malware applications, because they implement new databases that contain recently discovered threats and the fixes for them.

Therefore, anti-malware software needs to be properly installed and maintained if they are going to even stand a chance of keeping systems secure.

5. **Lack of firewalls**
A firewall is a network security tool that can be configured to block data traffic from entering and leaving the network. For instance, it can protect data from being accessed from outside the network. While many modems or routers include firewalls, they are often not robust enough for business use.

What you need is a firewall that covers the whole network at the point where data enters and exits (usually before the routers). These are business-centric tools that should be installed by an IT partner like a managed services provider (MSP), in order for them to be most effective.

Call us today to learn more!

FEATURED PARTNER

Dell

Dell is an American multinational computer technology company that develops, sells, repairs, and supports computers and related products and services. Dell sells personal computers (PCs), servers, data storage devices, network switches, software, computer peripherals, HDTVs, cameras, printers, MP3 players, and electronics built by other manufacturers.

RJ2 SPOTLIGHT

Jeff Dunham

Support Engineer

Jeff Dunham has been working in and around technology since 2001. He got his start in the construction industry, working with installing Smart homes. In 2003 Jeff enlisted in the U. S. Navy. Stationed on the USS Kitty HAWK (CV-63). Jeff worked on radar, and navigation systems.

Prior to joining RJ2, Jeff was an integral part of a small IT firm focused on both residential and SMB developing a wide variety of skill sets in variety of different industries. Since joining RJ2 Technologies in 2017, as a Systems Engineer, Jeff has continued to developed his technical knowledge to become a go to asset for physical infrastructure, and Telephonic needs.

Fun Fact: While in the Navy Jeff was station in Yokosuka, Japan and was able to tour around the Asia Pacific.

BUSINESS PRESENCE

Protect Your Browser, Protect Your Business

In small- and medium-sized businesses (SMBs), some 50 to 150 workers access the net daily through the company network via browsers. That's why any SMB must secure its browsers to keep its data safe from data theft and other forms of cyber attacks. To do so, follow these simple steps.

PREVENT BROWSER TRACKING

If you don't like the idea of a third party (reputable or otherwise) being able to track your browsing habits, enable private browsing using built-in tools in your internet browser such as Chrome's incognito mode. This offers protection against tracking by blocking third-party cookies as well as malware. Some browser extensions also boast secure Wi-Fi and bandwidth optimization and can guard against tracking and data collection from social networking sites such as Twitter and Facebook.

BLOCK ADVERTS

While online ads may seem harmless, the truth is they can contain scripts and widgets that send your data to a third party. A decent ad blocking program will stop banner, rollover, and pop-up ads, and prevent you from inadvertently visiting a site that may contain malware.
Many blockers contain additional features such as the ability to disable cookies and scripts used by third parties on sites, the option to block specific items, and options to "clean up" Facebook, and hide YouTube comments.

CONSIDER SETTING UP A VIRTUAL PRIVATE NETWORK (VPN)

Unfortunately, browser tracking and adware are not the only internet nasties that you need to be concerned about. Hackers can intercept sensitive data between two parties, allowing them to steal and corrupt valuable information such as bank details, login credentials, and other personal information. Installing a VPN can help solve this problem. VPNs encrypt your internet traffic, effectively shutting out anyone who may be trying to see what you're doing.

INSTALL ANTIVIRUS AND ANTI-MALWARE SOFTWARE

Finally, it goes without saying that having antivirus and anti-malware software installed on your PC, tablet, and smartphone is crucial if you want to ensure your online safety. These software programs are your first defense against malicious parties intent on stealing your data.

Is browsing at your workplace secure? Would you like a more comprehensive security system for your business? We can tell you all about it and help protect your business from online threats. Get in touch with us today.

10 EASY WAYS TO DEFEAT STRESS AT WORK

1. Take a walk. A 15-minute walk will refresh your mind.

2. Work outside. Weather permitting, working in the sun can boost your mood.

3. Meditate. Use a meditation app like Calm or Headspace to lower blood pressure and de-stress.

4. Take deep breaths.

5. Make a checklist. Write it out and focus on one task at a time.

6. Talk to a friend. Have a conversation about a problem. Talking it out can change your perspective.

7. Watch an informative video. It can be on anything. Videos are a great distraction for 5-10 minutes.

8. Listen to soothing music.

9. Take a 20-minute nap. Nothing does wonders for stress like a power nap — just be sure to set a timer!

10. Trust your instincts. If you feel you need a break, take it. Don't push yourself if it isn't necessary.

December

"It is December, and nobody asked if I was ready.
-Sarah Kay

CALENDAR OF EVENTS

Dec 24th: Christmas Eve Office Closed
Dec 25th: Christmas Day Office Closed
Jan 1st: New Year's Day Office Closed

RJ2 Technologies will be closed from 8 am to 5 pm on December 24th (Christmas Eve), December 25th (Christmas Day), and January 1st (New Year's Day). If there are any issues that arise during this period, please call: 847-303-1194. Rates are adjusted to incorporate the holiday hours.

Happy Holidays!