ISSUE 31 SUMMER 2020

RJ2 TECHNOLOGIES

Newsletter

What's Inside

If you haven't invested in IT security, then your business is at risk.

These days, it's easy to take technology for granted. It just seems like everything works so well. If things are working well, why spend more on things like data monitoring or secure cloud storage?

Here's a startling fact: a lot of business owners take this approach to network security. They might think, "This will never happen to me," when it comes to data breaches, malware and hacker attacks. While they might be great at running their businesses, they may end up skimping on their IT security.

They see it as something they simply don't need to invest in. But a lot of business owners end up paying big because they aren't serious enough about IT security. A simple virus scan app or firewall just isn't enough. Hackers and cybercriminals are relentless.

Here's another startling fact: threats like data breaches, malware and hacker attacks are a lot closer than you think. When you go cheap with your network security or don't work with an experienced IT services company, it can end up costing you big in the long run.

A lot of business owners skip out on things like network security, cloud backup, data protection and data monitoring because they don't like the up-front cost or another monthly bill. In reality, while you can expect an ongoing cost, working with a managed IT services firm can be remarkably cost-effective (and smart!).

When your network security solutions are running smoothly, you won't know it. It all happens in the background. But because it's not something you "see" on a daily basis, you might wonder if you're really getting your money's worth. This can be a challenge for business owners who may want to see tangible results for something they pay for. The good news is that you can get tangible results!

Here's why it can be so costly to NOT invest in IT security:

SCENARIO 1: Imagine you're hit with a malware attack, and it takes your network out of commission. Customer data is at risk, and your business comes to a screeching halt. You have to call in IT experts to fix the problem ASAP. This is a break-fix approach to IT services.

In this event, you're going to be charged BIG to get your business up and running again. The IT specialists will have to scrub your network and make sure everything can be recovered. Not only do you have to pay to get your network cleaned, but your cash flow also takes a hit while you wait around to get everything fixed.

SCENARIO 2: You're hit by a data breach. Hackers are looking for information they can exploit, such as credit card numbers, passwords and other identifying information. They often sell this information to other cybercriminals. In almost every case, this information CANNOT be recovered. Once it's gone, it's gone.

This means you have to take action FAST to make sure stolen information cannot be used. This includes changing credit card information and updating passwords. In the event of a data breach, the sooner you inform your customers, the better. But this is a double-edged sword. Your customers need to know so they can protect themselves. At the same time, your customers may lose faith in you because you put their data at risk.

These are just two examples out of many. When you don't take IT security seriously or you're cheap with your technology, it can end up costing you BIG in the end. Work with an IT security company that will work with you to protect your business the right way – and help you avoid scenarios just like these.

Contact RJ2
(847) 303-1194

Corporate Office
1900 East Golf Rd.
Suite 600
Schaumburg, IL 60173

Chicago Office
333 S. Wabash Ave
Suite 2700
Chicago, IL 60604

CYBERSECURITY

What Private Browsing Can and Can't Do

As you surf the web, it's nearly impossible to keep your internet activity completely private. Certain websites collect personal information for marketing purposes and your browser keeps track of all the websites you visit. That browsing information can also fall into the wrong hands, which is why you should consider using private browsing if you want to keep your online activities to yourself.

WHAT IS PRIVATE BROWSING?

Your web browser — whether it be Chrome, Edge, Firefox, Safari, or Opera — remembers the URLs of the sites you visit, cookies that track your activity, passwords you've used, and temporary files you've downloaded.

This can be convenient if you frequently visit certain pages, can't remember your login details, or if you're trying to recall a website you visited a few days ago. But if someone else uses or gains access to your computer, your most private (and embarrassing) internet activities are exposed for anyone to see.

With private browsing — also called Incognito Mode in Chrome and InPrivate Browsing in Edge — all the information listed above does not get recorded. In fact, all the websites and information you accessed in the private browsing session are immediately discarded without a trace as soon as you close the browser. This can come in handy when you're using a public computer because you're instantly logged out of all the accounts you accessed after closing the window.

Your cookies also won't be tracked. In a normal browsing session, sites like Facebook will display highly targeted ads based on the sites and pages you've visited. But in private browsing mode, your internet activity can't be tracked by marketing companies.

Another benefit of private browsing is that you can use it to log in to several accounts on the same site, which is useful if you need to log in to two different online accounts at the same time.

WHAT ARE THE LIMITATIONS OF PRIVATE BROWSING?

Although private browsing does prevent your web browser from storing your data, it doesn't stop anyone from snooping on your online activities in real time. If your computer is connected to the company network, system administrators can still track what you're browsing, even if you're in Incognito Mode.

Also, if spyware or keylogger malware is installed on your computer, hackers will still be able to see what you're doing online. Even though private browsing has quite a few benefits, you shouldn't solely depend on it for online privacy. Instead, you should use a virtual private network (VPN) when you go online. These encrypt your internet connection and prevent anyone from intercepting your data. And don't forget to use a strong anti-malware program to scan your computer and keep spyware and other malicious web monitoring software at bay.

RJ2 SPOTLIGHT

Kevin Dann

Dispatcher / Support Technician

Kevin Dann has been in the professional field since 2012. He started his career in the telecommunications field working as a project designer for Fullerton Engineering. Kevin joined RJ2 as an intern from 2010-2012 working onsite with engineers to develop technical profiles. In 2019 he became a full-time employee at RJ2 as a Dispatcher / Support Technician.

Fun Fact: Kevin once met actor Zachary Levi out in downtown Chicago

FEATURED PARTNER

VMware, Inc. is an American company that provides cloud and virtualization software and services, and claims to be the first to successfully virtualize the x86 architecture commercially. Founded in 1998, VMware is based in Palo Alto, California.

www.vmware.com

Feature Partner Product: Cloud Solutions

Access any cloud while maintaining the highest level of consistency for infrastructure, operations and developer experience.

With VMware, you have the freedom to build and deploy modern applications, from the data center to multiple cloud and edge environments. Migrate seamlessly between environments and ensure that all data and applications remain secure and protected in any cloud.

Match your applications to the unique strengths of any environment. With the most hybrid cloud options—delivered with key partners like AWS, Azure, Google Cloud, IBM Cloud and Oracle Cloud—you can access the power of leading hyperscale clouds within proven VMware infrastructure.

BUSINESS

7 Easy Ways to Prevent Data Loss in Microsoft 365

1. TAKE ADVANTAGE OF POLICY ALERTS

Establishing policy notifications in Microsoft 365's Compliance Center can help you meet your company's data security obligations. These preemptive warnings can prevent data leaks and also educate users on safer data sharing practices.

2. SECURE MOBILE DEVICES

Since personal smartphones and tablets are often used to access work email, calendar, contacts, and documents, securing them should be a critical part of protecting your organization's data. Installing mobile device management features for Microsoft 365 enables you to manage security policies and access permissions/ restrictions, and remotely wipe sensitive data from mobile devices if they're lost or stolen.

3. USE MULTIFACTOR AUTHENTICATION

Don't rely on a single password to safeguard your Microsoft 365 accounts. To reduce the risk of account hijacking, you must enable multifactor authentication.

4. APPLY SESSION TIMEOUTS

Many employees usually forget to log out of their Microsoft 365 accounts and keep their computers or mobile devices unlocked.

5. AVOID PUBLIC CALENDAR SHARING

Microsoft 365's calendar sharing features allow employees to share and sync their schedules with their colleagues'. However, publicly sharing this information is a bad idea because it helps attackers understand how your company works, determine who's away, and identify vulnerable users.

6. EMPLOY ROLE-BASED ACCESS CONTROLS

Another Microsoft 365 feature that will limit the flow of sensitive data across your company is access management. This lets you determine which user (or users) have access to specific files in your company. For example, front-of-house staff won't be able to read or edit executive-level documents, minimizing data leaks.

7. ENCRYPT EMAILS

Encrypting classified information is your last line of defense against data breaches. If hackers intercept your emails, encryption tools will make files unreadable to unauthorized recipients. This is a must-have for Microsoft 365, where files and emails are shared on a regular basis.

While Microsoft 365 offers users the ability to share data and collaborate, you must be aware of potential data security risks at all times. When you partner with us, we will make sure your Microsoft 365 is secure. If you need help keeping up with ever-changing data security and compliance obligations, we can assist you there, too! Contact us today for details.

August

" The ultimate promise of technology is to make us master of a world that we command by the push of a button."
- Volker Grassmuck

TIPS OF THE MONTH

Maximize you efficiency with these Microsoft Outlook tips:

1. **Organize your inbox**
2. **Ignore conversations**
3. **Send links to files**
4. **Schedule a teams meeting**
5. **Tag contacts**