ISSUE 23 FALL 2019

Newsletter

What's Inside

3 Things You Should Absolutely Demand From Your IT Services Firm

How much do you rely on your IT services provider? It's startling to think that a lot of small businesses outsource their IT (which is a good thing), only to get little to nothing out of that relationship.

Why is that?

Well, some businesses just aren't proactive. They only rely on their IT services company when something goes horribly wrong. If there's a network failure or their website gets hacked, they'll make the call to their IT people, but that's the extent of the relationship.

1: business owners should work closely with their IT pros. They should have the staff and resources to not only address your IT emergencies but also to keep your business safe and secure to minimize those emergencies. Here are four things you should ask of your IT services provider.

2: "Keep my business safe!" Your IT company should make sure your network security, firewalls, malware protection, etc., are installed, operating and up-to-date. They should be working with you to do everything to keep your business's data secure and make sure it can be restored in the rare event that data loss does occur.

Keeping your customer data secure should be a top priority. Don't take unnecessary risks, because when you do, the consequences can be devastating.

3: "Help me stay proactive!" An experienced IT company can often spot an issue before it becomes an issue. They keep your network updated and maintained, and they can help you avoid unnecessary downtime. Working closely with your IT company means you aren't skimping on security, and this alone puts you ahead of so many other businesses that do.

If your IT company isn't doing any of these things, you need to get on the phone with them NOW! Don't put your business at risk because you only make the call after the worst-case scenario has occurred. Call RJ2 Today for a Free Assessment Offer!

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

Protect Your Android Device

Protecting your Android device doesn't have to cost you a fortune. Why spend more for its protection when there are free ways to do it? Our guide will help you find ways to safeguard your phone or tablet without having to spend a lot.

Protecting your Android device from digital risks and theft should be a priority as most hackers continue to exploit Android's vulnerability. However, you don't need to purchase expensive software to safeguard your device. Most of the best protection against common Android threats is available for free.

Here are ways to secure your Android devices.

BUY DEVICES FROM VENDORS WHO RELEASE ANDROID PATCHES QUICKLY

Beware of handset makers who don't immediately release Android updates. By delaying the patches, these vendors allow your device to be vulnerable for the time being.

ALWAYS KEEP YOUR SOFTWARE UPDATED

Google releases security patches fairly regularly, and most newer phones automatically inform you of updates. Update your device and apps as soon as security patches are released.

MAKE SURE TO LOCK YOUR SCREEN

You can lock and unlock your Android device's screen in multiple ways. These provide an extra layer of protection as they require you to unlock a device with either a unique code, pattern, or face recognition.

The simplest way is to use a personal identification number (PIN); however, make sure you don't use 1-2-3-4-5 or some easy-to-guess combination. For newer Android devices, you can set up a fingerprint unlock.

DOWNLOADS APPS ONLY ON GOOGLE PLAY STORE

Google Play is the safest place to download apps for your device. Third-party sites may offer an interesting lineup of apps, but these can be malicious and certainly not worth the risk.

Sometimes bogus apps make it into the Google Play Store, so always read reviews before downloading apps. These will usually tell you if an app is legitimate.

USE ON-DEVICE ENCRYPTION

This feature encrypts all your device's sensitive data, rendering them unreadable until you enter your PIN or passcode. Activate it by going to Settings > Security > Encrypt Device.

USE A VIRTUAL PRIVATE NETWORK (VPN)

When connected to public Wi-Fi, there's always a possibility that someone connected to the same network is intercepting your connection. Using a VPN encrypts your information, so even if someone steals it, it's protected.

There are numerous VPNs on the Google Play Store that are free and simple to use. Compare their rankings and reviews before picking one.

Call RJ2 if you have any questions about your Android Device. We are here to help!

FEATURED PARTNER

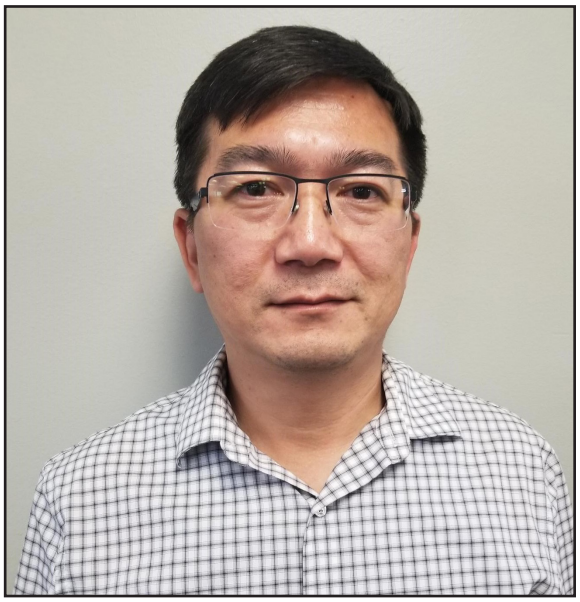
VMWARE

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.

RJ2 SPOTLIGHT

Di Zhang

System Engineer



Di Zhang has been in the IT professional field since 2001, he graduated from Tianjin University (Tianjin, China) in 1995, started his career as an electrical engineer and switched to IT engineering. Before coming to RJ2, he was working with another MSP/ IT company for 17 years.

Di joined RJ2 Technologies in 2018, as a field ngineer, providing onsite and remote support services for clients.

Fun Fact: Di enjoys yard work at home and grows his own vegetables such as tomato, cucumber, pepper and squish.

BUSINESS PRESENCE

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.

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. With fairly simple tools and a bit of know-how, hackers and criminals can start capturing data that goes in and out of the network, and even attacking the network and computers attached.

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.

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.

The same goes for not properly ensuring that these systems are updated. 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.

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.

HOW DO I ENSURE PROPER BUSINESS SECURITY?

The best way a business can ensure that their systems and networks are secure is to work with an IT partner like us. Our managed services can help ensure that you set up proper security measures in place and that they are managed properly. Tech peace of mind means your focus can be on creating a successful company instead.

Contact us today to learn more!

Featured Product:

VMWARE Products:

VSphere: Industry-leading server virtualization platform; the ideal foundation for any cloud environment.

VMware Enterprise PKS: Production-grade Kubernetes for multi-cloud enterprises and service providers.

VCloud Availability for VCloud Director: vCloud Availability for vCloud Director enables VMware Cloud Providers to offer simple, cost-effective cloud-based disaster recovery services.

VCenter Server: Centralized platform for managing vSphere environments across hybrid cloud.

November

"The science of today is the technology of tomorrow. " - Edward Teller

CALENDAR OF EVENTS

Nov 28-29: Thanksgiving and Black Friday

RJ2 Technologies will be closed from 8 am to 5 pm on November 28th (Thanksgiving) and November 29th (Black Friday). If there are any issues that arise during this period, please call: 847-303-1194. Rates are adjusted to incorporate the holiday hours.

Have a Happy Thanksgiving!