ISSUE 37 WINTER 2021

Newsletter

What's Inside

Fix these business security flaws now

As businesses have become more reliant on technology, they've also become a prime target of cybercriminals. If you want to protect your organization from cyberattacks, make sure your cybersecurity system doesn't have the following flaws.

OPEN WIRELESS NETWORKS

With just one main internet line and a couple of wireless routers, an entire office can get online. A wireless internet connection saves money, but there's a risk that it might be unsecure.

UNSECURE EMAIL

Most companies that have implemented a new email system in the past couple of years are most likely secure. This is especially true if they use cloud-based platforms or well-known email systems like Exchange, which offer enhanced security and scanning.

UNSECURE MOBILE DEVICES

Mobile devices help you stay connected and productive while out of the office. However, if you use your tablet or smartphone to connect to office systems without proper security measures in place, you run the risk of compromising your networks.

ANTI-MALWARE SOFTWARE THAT ISN'T PROPERLY MAINTAINED

Anti-malware software needs to be properly installed and maintained if they are going to stand a chance of keeping your systems secure.

LACK OF FIREWALLS

A firewall is a network security tool that filters incoming and outgoing network traffic and protects data from being accessed from outside the network. While many modems or routers include firewalls, they are often not powerful enough for business use.

HOW DO I ENSURE PROPER BUSINESS SECURITY?

The best way to secure business systems and networks is to work with an IT partner like us. Our managed services can help you set up cybersecurity measures and ensure that they are managed properly. Tech peace of mind means you can focus on growing your business. Contact us today to learn more.

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

Picking the right office Wi-Fi router

Selecting a Wi-Fi router, much like selecting any other piece of equipment for your business, can be a complicated task. The sheer variety of models available can make it difficult to choose the best option. However, if you know what features to look for, it's much easier to make the right decision.

NETWORK TYPE
Look at any router and you will quickly see that there are a number of different network types available. Also referred to as wireless protocols, the four most common types are 802.11b, 802.11g, 802.11n, and 802.11ac. These designations indicate how fast the router can transfer wireless data, with 802.11ac being the fastest.

Newer routers now utilize the latest Wi-Fi protocol dubbed 802.11ax. Also known as Wi-Fi 6 or High-Efficiency Wireless (HEW) , this new protocol improves upon 802.11ac tech in the following ways:

- Greater throughput speeds (up to 9.6 Gbps)
- Reduced network congestion and expanded client capacity, thanks to Orthogonal Frequency-Division Multiple Access (OFDMA)
- Improved range performance
- Reduced power consumption by network-connected devices, courtesy of Target Wake Time (TWT)
- OFDMA enhances network performance by splitting up Wi-Fi channels into sub-channels. Doing so permits up to 30 users to use the same channel simultaneously.

TWT reduces the power consumption of connected devices by allowing them to determine when and how often they will wake up to begin sending and receiving data. This extends the battery life of smartphones and battery-powered internet of things (IoT) home devices such as smart thermostats and security cameras.

THROUGHPUT
In communication networks, throughput is the rate at which messages are successfully delivered via a communications channel. A router's throughput, in particular, is the speed at which the router is supposed to transmit data from your connection to users. To spot the router's throughput, look for Mbps (or Gbps for its cable ethernet connections). It is usually one of the first things listed on router boxes and specifications.

Keep in mind that if you have a 100 Mbps internet connection, but your router can only deliver up to 80 Mbps, then the total speed of your network will be the lower figure. Therefore, it would be best to get a router with a higher throughput if your internet service provider delivers faster connections.

BANDS
On every single router's box, you will see numbers like 2.4 Ghz and 5 Ghz. These indicate the wireless radios on the router. A dual- or tri-band router will have both radios so that the connection workload can be split between them.

The 2.4 Ghz radio is sufficient for activities that don't require much network bandwidth, such as web browsing and replying to emails. Since its band is of a lower frequency, it reaches farther than 5 Ghz but is more easily blocked by concrete walls.

The 5 Ghz band, on the other hand, has greater power, but has a shorter broadcast range. 5 Ghz is what you'll want to use for video conferencing and playing online games (if permitted by the company after office hours, of course).

MULTIPLE INPUT, MULTIPLE OUTPUT (MIMO)
MIMO is the use of multiple antennas to increase performance and overall throughput. MIMO-enabled routers ensure that more devices can connect to one router with less interference.

When it comes to real-world tests, there is often a slight improvement if the antennae are configured and aimed properly. However, getting a high-end router with six or more antennae may be an unnecessary cost for small businesses.

BEAMFORMING
Beamforming is a feature that's now standard in mid- to high-end routers. It is a form of signal technology that allows for better throughput in areas with poor or dead signals. In other words, it can help improve the connection quality with devices behind solid walls or in rooms with high amounts of signal interference.

QUALITY OF SERVICE (QOS)
QoS allows the router administrator to limit certain types of traffic. For example, you can use the QoS feature of a router to completely block all torrent traffic, or limit it so that other users can have equal bandwidth. Not every router has this ability, but it is a highly beneficial feature for office routers.

There's a lot to consider when it comes to picking a router, which is why we recommend you contact us. We can evaluate your networking needs and help you find the best setup for your business.

RJ2 SPOTLIGHT

Lauren Wood

Client Success Manager

Lauren Wood has been in the professional field since 2016. She is a Business graduate from Concordia University - Wisconsin. She started her career in the healthcare field working for Northwest Community Hospital. Before coming to RJ2 she was an account manager at Young Innovations, located in Algonquin IL.

Lauren joined RJ2 Technologies as an intern from 2013-2015. In 2017 she became a full-time employee at RJ2 as an Executive Assistant to the President, Jeff Dann. Additional duties include Marketing Specialist and Account Management.

FEATURED PARTNER

As your needs grow and change over time, so do our features and capabilities. Endlessly scalable, flexible, and reliable, our cloud communications platform is truly future-proof, so you can focus on your business, and know that your communications solution will always remain relevant and competitive.

Feature Partner Product: SkyCom

Unified Communications

Unified Communications (UC) is the seamless integration of voice, presence, chat, data, applications, and other technologies that help drastically improve your communication processes and business productivity. Our software and services enable you to access your account and seamlessly incorporate our high-value cloud communication services.

Hosted PBX & VoIP

You want a reliable, high-quality phone system that simply works. And so you can focus on your business, and not your communications platform, our system adapts and adjusts to your needs and seamlessly works the way you do. Whether you have five (5) or five hundred (500) employees, we have a solution that meets your needs.

Virtual Auto Attendant & Mobile VoIP

Use auto attendants, cloud extensions and mailboxes to stay connected with your customers and employees—with all the features of a high end phone system. Best of all, you can seamlessly connect mobile and home workers with current or future office locations. It's all the same cloud communications framework, so you can scale up as needed, and connect based on your specific business requirements.

BUSINESS

How to prevent VoIP theft of service

Voice over Internet Protocol (VoIP) phone systems allow users to make and receive calls using the internet instead of traditional phone lines. This presents many advantages ranging from better call quality to lower costs. However, VoIP also has several disadvantages, one of which is that hackers can use VoIP phones to gain access to an organization's servers and data through a type of fraud known as VoIP theft of service.

WHAT IS THEFT OF SERVICE?

VoIP theft of service is the most common type of VoIP fraud. At its most basic level, it involves the theft of your organization's VoIP account credentials, including usernames and passwords, either by eavesdropping or by introducing malware into your system. Once cybercriminals gain access to your account, they can freely make phone calls or change your call plans, running up your VoIP bill.

In addition, cybercriminals may use the stolen data to carry out other fraudulent activities. They can also use theft of service to flood your VoIP network with promotional calls similar to junk email via an attack called spam over internet telephony, or SPIT. Once they infiltrate your communications network, they might broadcast unsolicited messages or advertisements over your VoIP system. This keeps users from making or receiving calls, which can have a significant impact on your business's operations.

HOW CAN YOU AVOID THEFT OF SERVICE?

Preventing VoIP theft of service simply requires using a little common sense and implementing some technical preventive measures.

1. Make your passwords as secure as possible. Passwords must be 8–12 characters long, consisting of a combination of upper- and lowercase letters, numbers, and symbols. For added security, use passphrases, which are sentence-like strings of words. They're usually longer than passwords, easier to remember, and more difficult to crack.
2. Install firmware patches for your VoIP phones and infrastructure regularly, and keep your antivirus software up to date.
3. Use fraudulent call routing detection and encryption software.
4. Set up an enterprise-grade virtual private network (VPN) for employees working from home. A VPN encrypts incoming and outgoing traffic without compromising call quality.
5. Review your organization's call logs for any unusual trends or behavior, such as higher-than-usual call volumes or calls made during off-hours.
6. VoIP is an essential business communication tool, so it makes sense to understand what theft of service is to avoid its impacts on your company's operations.

February

"What new technology does is create new opportunities to do a job that customers want done."
- Tim O'Reilly

TIPS OF THE MONTH

Avoid Cybercrime in 2021 With 8 Helpful Tips

1. **Install antivirus and firewall protection**
2. **Adopt multi-authentication protocols**
3. **Avoid the usage of public WiFi**
4. **Regularly backup system data**
5. **Avoid the insertion of foreign USB devices into the company computers**
6. **Educate employees on Cyber Security threats**
7. **Regularly update all software and operating systems**
8. **Regularly update passwords**