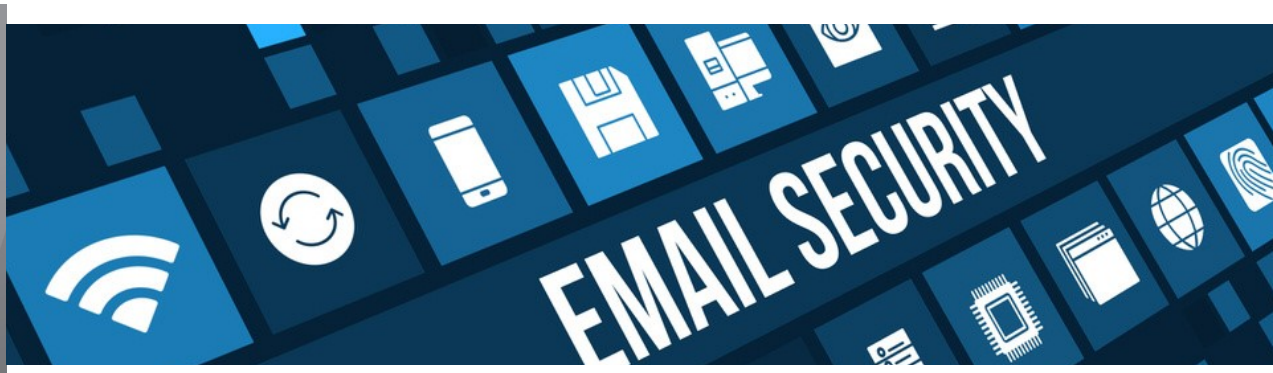
E-NEWS

January 2019

In this issue…



Comprehensive Email Protection

It's 2019 and E-Mail protection is as important as ever!

Email continues to be the single biggest source of cyber-attacks globally. A recent survey* estimated that in 2017, 74% of threats initially entered organizations via email.

The traditional approach to email security blocks spam and malware at the gateway before it enters an organization and enforces policy controls at this point. This approach is still necessary but is not able to secure against advanced email threats such as spear phishing attacks, account takeover, business fraud and data loss.

Barracuda Email Protection provides a comprehensive solution that secures your entire email infrastructure. The multi-layered approach covers all threat vectors by securing the email gateway, protecting your stored email data, inoculating mailboxes against targeted threats, and training users on how to identify and defend against cyber-attacks.Providing a comprehensive solution to defend against the full range of email threats that organizations are now facing is a complex and rapidly evolving multi-dimensional challenge.

Barracuda's suite of purpose-built security solutions builds on years of experience and leverages a global network to provide an easy, economical, scalable, and powerful way for organizations to address this challenge.

Be sure to contact us today and find out how we can help you be proactive against email threats!

Get Your Network Gear Ready with UPS

Clever business owners utilize an uninterruptible power supply (UPS) during disasters like fires, storms, and other emergency situations. A UPS is usually set up for desktop computers to give users enough time to save their work and progress. Another useful power-saving plan for emergency situations would be to use a UPS for networking gear.

UPS for network equipment

UPS systems provide backup power in case of outages and protection against power surges, which don't just damage computers but also make you lose unsaved work. Deploying them for Wi-Fi routers and modems allows you to stay connected to the internet during these typically chaotic instances.

Moreover, it makes sense to not just keep your PCs powered up, but to also have internet access during a disaster. This strategy works relatively well if your staff are predominantly laptop users, as that means you only need to juice up your Wi-Fi gear.

Better than generators

Although generators are indispensable for certain businesses, they also require greater upkeep. Small- and mid-sized businesses may not have enough capacity to maintain them because they typically require a utility crew who can manage high-maintenance equipment.

What's more, misusing or mishandling generators could result in generator-related fatalities. On the other hand, misusing a UPS unit could result in the loss of a day's work, but it's unlikely to lead to anything as extreme.

Why internet access is important during a disaster

UPS-supported modems or routers help you stay online for as much as 90 minutes, which should be enough time to get your bearings before power finally runs out. Internet service providers are usually prepared for catastrophes and would normally have an emergency power source to stay operational. And if you can stay online via Wi-Fi during an emergency, you get the following benefits:

- Internet speed that's faster than cellular access
- No extra telecom costs resulting from overreliance on cellular data
- All devices stay online using a stable Wi-Fi connection
- Devices don't have to rely on cellular data-equipped phones for internet connection

Plug in your network gear now

Businesses that aren't located in disaster-prone areas probably don't give much thought to installing UPSs for their computers, let alone their modems. But accidents and emergencies are inevitable. And when they happen, you'll find that having internet access is one of the most important things you need to ensure business continuity.

Think of an emergency power supply source like a UPS as an investment that not only protects your systems from data loss but also keeps your Wi-Fi equipment functioning in emergency scenarios. Call us today for productivity-saving tips and other hardware hacks for your business.

.

Use Virtualization to Protect your Devices

Cybersecurity threats are increasing for both small and large businesses, which means solutions that protect mobile devices are no longer just nice-to-have solutions. As more work is handled outside of the office, the risks to your data increase. Virtualization vendors are leading the charge to tackle these challenges with innovative solutions.

Mobile device management and virtualization

Mobile device management (MDM) is about controlling how users on any device — from laptops to internet-connected printers — view, share, and store sensitive information.

For example, if you have a user who accesses data via a company-provided laptop, an office copier, and a personal smartphone, IT administrators can install an application on each device to enforce policies from a centralized console.

There are dozens of standalone MDM solutions that consolidate device administration, but by using one that integrates with your virtualization platform, you can standardize policies for any industry across a range of company-owned, line-of-business, and personal devices.

Users are constantly picking up and discarding devices. Solutions like VMware's AirWatch and Citrix's XenMobile mean you no longer need to manage security settings for each device; instead, you can configure one virtualized environment for one employee, and its settings will be applied regardless of which device it's accessed from.

What are the benefits?

Beyond a centralized approach to device management and data access rights, virtualized MDM solutions allow you to enjoy a number of other benefits. For example, IT administrators can remotely lock or erase data on employee devices if the device has been lost or stolen.

You can also benefit from Single Sign-On security. This means your users need only one set of login credentials to access all their applications. Technically, each application will still use a different username and password, but your virtualized solution will securely store each of the credentials and automatically log in users whenever they sign in to your MDM platform.

Hardware and software are evolving so fast that it's almost impossible to secure them without extensive IT training. With a little help from trained professionals, virtualization is one of the easiest and most cost-effective ways for business owners to simplify user settings and management.

It only makes sense that the next step would be unifying virtualized desktops, laptops, smartphones and other mobile devices under a single solution. Call us today to get started.

VPNs: Why You Need Them

Installing antivirus software and setting strong passwords are no longer considered the bare minimum in cybersecurity. With hackers, third parties, and ISPs constantly monitoring networks and your online habits, hopping onto a virtual private network (VPN) is crucial for keeping your surfing habits private. Here's why.

What is a VPN?

The best way to describe a VPN is as a secure tunnel between your device and destinations you visit on the internet. Once you've established your PC's connection to a VPN server, your computer acts as if it's on the same local connection as the VPN making it seem you moved to a different location. As far as websites are concerned, you're browsing from that server's geographical location, not your computer's actual location.

When you surf the web through a VPN, all the data transmitted and received is also encrypted, preventing anyone — from hackers to government agencies — from monitoring your online activities.

Why should you have one?

Of course, security and privacy are major reasons why you would want a VPN. For example, if you're connected to a public Wi-Fi network — like the ones you typically encounter at local cafes and airports — using a VPN encrypts the information you're sending or accessing online. This means your credit card details, login credentials, private conversations, or other sensitive documents can't be intercepted by a third party.

VPNs are also useful for accessing geo-restricted websites. If you're traveling abroad and certain US websites are blocked in that region, you can connect to a VPN located in the US to access the sites you need.

Which VPN should you choose?

Given the increasing demand for secure online privacy, VPNs are surging in popularity. The following considerations can help you find the right one.

1. Cost
While free VPNs are available, we strongly suggest you avoid them as they could keep logs of your internet activity, and in some cases sell them to data brokers or worse, cybercriminals.

Maintaining a VPN service is also expensive, which means the free ones will likely plaster ads on your browser to make a quick buck.

Paid VPNs like SurfEasy and StrongVPN often come with more robust features and configurations that keep you secure. Prices differ depending on a VPN's features and subscription length, and remember that how you pay is also important. Some VPNs offer anonymous payment systems like bitcoin while others allow you to use gift cards to avoid giving out your personal information.

2. Location
The physical location of VPN servers is important if you want to access region-blocked websites. So if you're planning on accessing a UK-based service, your VPN provider must at least have servers installed in London.

3. Capacity
Read through a VPN provider's terms of service to determine how much data you're allowed to use. If possible, find out how many servers a VPN provider has. If they have plenty of servers online, you can rest assured that they have the capacity to support your internet browsing.

4. Device compatibility
Another important factor to consider is whether the VPN can be used across multiple devices. Nowadays, employees work on laptops, tablets, and smartphones, so you'll want a VPN that's compatible with all these.

5. IP leaking
Beyond the fundamental nuts and bolts of the VPN protocol, there are other challenges like dealing with leaky tunnels, which means your IP address could be tracked. A great way to evaluate a VPN service is to sign up for their free trial service and visit https://ipleak.net. This will allow you to check whether your real IP address is actually being leaked. If it tracks your physical location, you should opt for a more reliable VPN service.