August 2023

IT Radix Resource

We make IT work for you

IT Security Commandment #6:
Thou Shalt Manage Access Securely

It is late in the evening, and you are snoozing on the couch. Your phone rings unexpectedly and wakes you. You pick it up, "Hello?" and an unrecognizable voice says, "Help me! I am at your front door, can you let me in your door right now?" What would be your response? Most likely it would be, "Who is this!?" And, hopefully the person identifies themselves as someone you know as you run toward the door to look through the peephole. You are intrinsically performing identity authentication. You are making sure you know who it is, so you don't inadvertently let someone with nefarious motives into your home. Smart move!

Multi-Factor Authentication (MFA) Adds a Security Layer

Doing the same thing as it relates to access to your organization's network, software, data, and equipment ensures that you are complying with the 5th Commandment of IT Security which is: *Thou Shalt Manage Access Securely*. In other discussions of the 10 Commandments of IT Security, we have mentioned a number of ways to manage secure access—everything from passwords, to encryption, to how to manage "permissions" to certain folders/files in your network, to simple laptop locks. But this commandment focuses on authentication—specifically Multi-Factor Authentication (MFA). Our point of view is if MFA can be implemented for every service/program you log into, it should be.

Multi-Factor Authentication adds an incremental layer of security beyond usernames and passwords to limit access to systems and software. In simple terms, whenever a user attempts to access something, a unique code is sent to the computer or smartphone of that user. The user must then input that code in order for access to be granted. The reason this layer is valuable and works well is that it reduces the risks associated with thefts of credentials and duplicate/weak passwords used across various systems. Google security reports that putting MFA in place can prevent over 95% of bulk phishing attempts and over 75% of targeted attacks.

Implementing MFA is fairly easy. It is an extra step that staff members must come to accept and recognize the value it brings. There is usually a

(Continued on page 2)

Take Note

September 27
WEBINAR
10-Minute Tech Talk:
Zero Trust Starts Now!
www.it-radix.com/webinar
Starts @ 12:10pm sharp

Windows Server 2012 EOL
Windows Server 2012 will reach its end of life on October 10th. With no security patches beyond this date, your applications and data will be vulnerable—putting your company at risk. No time like the present to make plans before it's too late.

If you would rather receive our newsletter via email, sign up on our website or send an email to resource@it-radix.com

More free tech tips at:
www.it-radix.com/blog

Manage Access

(Continued from page 1)

nominal set-up cost and then an ongoing modest licensing fee per month per user. It is money well spent. Many organizations have smartly decided to put a cyber-liability insurance policy in place. Those insurers can attest to the value of MFA as they are now demanding it be in place for access to network systems, email, and key software (especially financial and accounting software). We recommend that anything that your staff uses every day that is proprietary or important should have MFA in place. We especially suggest that MFA be put in place for any user who has administrator access to the key server or key applications at your business—a requirement by cyber insurers.

So again, just think of MFA as another way of saying, "Who is there?" "Who is this?" and getting the right answer before you let anyone into your network. Do that and you are following the 5th Commandment of IT Security!

How Your Online Habits Impact the Planet

Have you ever really thought about the infrastructure required to send an email, store files, or have a video meeting? The technical infrastructure required to deliver these services and functionality are "out of sight, out of mind," and therefore, are often assumed to have a low environmental footprint. While digital services may not seem to negatively affect the environment due to their accessibility and low variable costs, they actually contribute significantly to greenhouse gas emissions and require heavy land and water use.

Cloud-based storage has a relatively low financial cost, but it does not reflect the high environmental costs involved. On average, data centers emit around 0.2 tons of CO_2 per year for every gigabyte of storage they offer. A good reason to take control of your digital hoarding and save only what's really needed. Quite often, we tend to keep everything "just in case." By thoughtfully considering what digital information you're storing, you can reduce the amount of infrastructure and save energy.

Switching from streaming in High Definition (HD) to Standard Definition generates 20 times less CO_2 annually. Surprisingly, mobile device communications are more energy intensive than laptop-to-laptop emailing.

Heavy users of computing, such as those using supercomputers or training AI models (e.g., ChatGPT), contribute significantly to carbon dioxide emissions. A standard supercomputer generates approximately 15 kilotons of CO_2 per year. Shifting to renewable energy could reduce this by about 96%. Encourage your government agencies and corporations to take responsibility for addressing their digital sustainability.

Changing our online habits can help save energy and reduce our environmental impact.

Service Spotlight: Reap the Benefits of Our Zero Trust Security Solution

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration before being granted or keeping access to applications and data. IT Radix offers a Zero Trust security solution that strengthens our clients' stance against cyberattacks. Here are a few benefits:

Zero Day Attacks: Protect against vulnerabilities that haven't even been discovered yet.
Ransomware: Ringfencing lets you dictate how apps interact with data—blocking any unauthorized use.
Per User Limits: Eliminate the need to grant blanket access. Instead, create policies for groups or unique users.
Monitor Access: See who is accessing your files and when with detailed reports generated in real time.
Restrict Applications: Let only trusted apps access your data, as determined by your custom policies.

Special Offer: 10% discount on setup of Zero Trust Protection through 8/31/23

Safely Using Technology to Run Your Office

Is the Internet the greatest cost reduction and energy saving device ever invented? It may well be!

We often think of the Internet as a source of information and/or a means of communication. But with the Internet of Things (the networking capability of the internet allowing for communication between devices), the Internet can now be viewed and used as an "appliance" or even "partner" to assist you in managing your office. The time to take advantage of this technology is now, but it's imperative that you also implement the necessary security precautions.

Leveraging this capability can be as simple as installing smart lighting and thermostat sensors. These detect a variety of factors—temperature, humidity, daylight, movement, $C0_2$ levels—and they continually adjust HVAC and electrical systems to optimize efficiency and minimize waste. Further investment in systems that store energy is another way to take advantage of these latest technologies.

Incorporating the above can make managing an office environment more efficient. However, since it relies on the Internet for ongoing communication of key data, it also exposes any site to the risk of an attack or a penetrating breach from nefarious elements. Therefore, the approach to implementing these efficiency devices must include a heavy dose of security. Going forward, physical and cybersecurity functions should be combined into one department or responsible individual. The time for two silos on this topic is behind us. The knowledge and collaboration needed to safely implement building management demands this approach.

Additionally, putting smart devices into your environment means that they need to be managed and monitored. The days of purchase it, install it, and leave it alone are over. Make sure you manage all of these applications and devices off of some sort of central platform that can keep you apprised of the need for hardware replacement, firmware, and security updates. It is vital for you to know how/when the endpoints in your locations are accessing the Internet. If you have a proper inventory of your systems and devices, enforce compliance with your security protocols, and monitor traffic, you will be well on your way to safely using technology to run your office.

If you want to learn more about this topic, let us know. IT Radix is here to make technology work for you!

3 Easy Ways to Make Your Mac More Secure

Data breaches and malware attacks on Macs have been on the rise over the past few years, so you must take the necessary precautions to protect your devices. Below are three easy ways to make your Mac more secure.

1. Install a mobile device management profile so you can give an administrator remote access to the device. If your Mac is ever stolen, you can locate it and lock it before any of your data becomes compromised.
2. Utilize Multi-Factor Authentication (MFA) which will require you to confirm your login on another device. This adds an extra layer of security to your Mac.
3. Back up your data to protect yourself from ransomware attacks. Consider buying an external hard drive or a cloud storage solution and backup software to do so.

Contact us for more security tips.

Welcome!

A warm welcome to our newest Management and Support clients:

Belair Holdings USA
Law Offices of William R. Connelly, LLC
Yodice & Company CPAs

IT Radix is here to service all of your technology needs!

IT Radix
We make IT work for you
49 S. Jefferson Road
Whippany, NJ 07981

Inside This Issue

- How to prevent over 95% of bulk phishing attempts and over 75% of targeted attacks
- How changing our online habits can help save energy and reduce our environmental impact
- How to manage an office environment more efficiently

IT Radix Family and Friends
321 Delighted Clients Drive
Geekville, NJ USA

"Nature provides a free lunch, but only if we control our appetites."
— William Ruckelshaus

From the desk of Cathy Coloff

As we enter the dog days of summer, I'm sitting on the patio behind our home enjoying the weather, the sounds of the birds, soft music on the outdoor speaker and just taking it all in. Sometimes you just need to kick back and do nothing—often a hard thing for me to do.

I love learning new things and playing with technology that enhances my life or work. There's been a lot of buzz about AI in the news and I've been lightly digging in to see what all the buzz is about. In June, we did a high-level webinar on ChatGPT. It was fun, cool and a bit scary to see a humorous poem about the team at IT Radix generated within a few seconds. Since I started playing with ChatGPT, I have used it primarily to get my own creative juices flowing and move past the "blank paper" syndrome. In truth, I used it to help me get started writing one of the articles for this newsletter. I didn't particularly care for much of what ChatGPT created but it helped me clarify what I did like and wanted to highlight.

Like it or not, AI is going to change our world… I can only hope for the good. Want to talk more about how to use ChatGPT in your world? I'd love to chat (pun intended).