June 2023

# IT Radix Resource

We make IT work for you

## IT Security Commandment #4:
## Thou Shalt Not Expose Thy Data

Q: Do you know why you should never stop exposing your IT staff to COVID and/or flu jokes?
A: It is the best way to achieve nerd immunity!

Now that we have your attention, let's discuss the fourth commandment of IT Security—*Thou Shalt Not Expose Thy Data*. In simple terms, the exposure of anything sensitive and/or confidential within your organization to the outside world can be a risk. This can include financial reports, bank account numbers, credit card information, usernames, passwords, customer records, health care data and so on. But, in truth, almost anything that is important or proprietary within your organization that you do not want released to the outside world should be protected and secured.

The first thing to do is a Strategic Exercise. The purpose is to identify important data across your organization and put in place policies and procedures to protect that data from both accidental exposure and from an outside attack. Each organization essentially has three kinds of data: a) financial records of the business, b) business property, which is everything from copyrights and patents to sales and marketing plans to customer and supplier information and so on, and c) personal identifiable information (PII) which is everything from birth dates to license plate numbers and everything in between. Each of these types of information should be evaluated to determine how accessible it should be within the company and how much it should be protected. This is the first step in creating a sound Data Access and Privileged Access Policy. This puts you on the road to never committing the sin of violating the 4th commandment!

Now let's review several tactics to put in place that lower the risk of data leaks or attacks:

**Encrypted Backups.** Backups are important, and the internet makes offsite backups even easier. But it is vital that all backups are encrypted because with any storage, local or in the cloud, there is risk of exposure. Encryption conceals the real information within a backup and maintains confidentiality.

**Avoid Public Wi-Fi and Use VPN.** It is risky to use any business device on a public wireless network. It should be avoided at all times. Many networks appear to be legitimate but are not, and even the legitimate ones are

*(Continued on page 2)*

## Take Note

June 7
WEBINAR
30-Minute Tech Talk:
**Exploring AI Opportunities for Your Business**
www.it-radix.com/webinar
Starts @ 12:10pm sharp

Earth Day E-Waste Results
We are excited to share that we collected and properly recycled over ten, 54-cubic-feet bins of e-waste during our April electronic recycling event.

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**

# Thou Shalt Not Expose Thy Data

*(Continued from page 1)*

usually not encrypted at all. In cases where such use is unavoidable, use a Virtual Private Network (VPN) tunnel or secure HTTP connection to keep things safe. Additionally, when working remotely with a wireless mouse, be aware that mouse jacking is possible. That is when a criminal uses an antenna to connect to your dongle enabling the wireless mouse to work. Try to use your touchpad instead!

**Separate Internal and Guest Wi-Fi Networks.** This is very important to reduce exposure within your own network. Guests or employee-owned smart phones often want to access a wireless network while at your location. Segmenting out a guest network for their use is a smart move. Keeping your guest Wi-Fi separate and isolated from your internal network is important to ensure unwanted users or devices are not able to gain access to parts of the network used by your internal systems.

**Multi-Factor Authentication (MFA).** Putting in place a policy and system software that ensures that an end user successfully identifies themselves in multiple ways before gaining access to a business site and/or business data is a crucial method to reduce security risks. It is an extra layer of protection. In our view, anything that can be protected by MFA should be!

**Password Management and Security.** With the requirement of passwords for everything coupled with the fact that these passwords should be complex, the need for an organization to put a Password Management System in place has arrived. Typically, cloud-based password management software keeps a secure, encrypted online database of all passwords and has an important logging/tracking function built in. Why? So that audits can be produced to identify who accessed passwords and when. The added benefit is that users only need to recall one password—the one to access the password management software—in order to gain access to all the credentials required to do their work.

**Activity or Event Logging.** While not always needed in every organization, firms with higher needs for security and detailed knowledge of activity will put in place event logs on their networks or cloud services. Historically, this was used to enforce worker productivity, but it has also become a way to record access to information as well as understand the scope of an incident.

**Awareness.** Nothing will work better than educating your staff and training them on how to properly secure your organization's data. In fact, it is a commandment in and of itself, so we will not belabor the point here. Just remember your staff, when aware, is a great layer of security because most breaches or leaks are caused by human error.

**Log Out!** Finally, make it a practice for yourself and your staff to log out whenever you have completed work within a program or on your device. Having too many websites and/or windows open on a screen and then forgetting they are there just leads to trouble. So, give yourself the joy of logging out and moving on whenever you complete something!

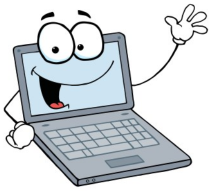
Remember this commandment because exposing your business data to the world is just plain indecent! Contact us today for more information on how to protect yourself and your team.

## Do NOT Save Passwords in Your Browser

While it's tempting to click *"Remember Password"* when your web browser prompts you, doing so is risky business. When you save this information, your web browser stores a database of logins and pre-populates the fields the next time you log in. Very convenient indeed!

**But here's the dark side…** This database of passwords stored in your browser is not secure. If hackers gain access to your computer, they could extract the contents of the database and get access to ALL your private logins. An automated, cloud-based password manager that can be used by all your staff working onsite or remotely is the solution!

Sign up in June for IT Radix's Password Management Solution
and get a Baker's Dozen—that's 13 months for the price of 12!



## Computer Power Tips

Did you know an idle PC uses 90 watts per hour? Compare that to a PC on standby mode, which consumes only 5 watts per hour. Configuring power-save settings properly on a computer can significantly reduce energy consumption and save electricity. The energy savings will depend on factors such as the specific power settings, usage patterns, and hardware configuration. Here are a few power saving tips from us to you:

**Sleep Mode/Hibernation.** Set up your PC's sleep mode or hibernation when the computer is idle to trigger after 15 minutes of inactivity. Automatically putting the computer to sleep or hibernation after a period of inactivity conserves power during those times.

**Display Settings.** Adjust the display settings, such as reducing screen brightness and the screen timeout periods, to ramp up your energy savings. Bonus: These settings will extend battery life on mobile devices.

**Power Plans.** Choose the appropriate power plan, such as the "Balanced" or "Power Saver" plan, to optimize performance and power usage based on your preferences.

**Power-Off Peripherals.** Turn off or disconnect peripherals like printers, external hard drives, or USB devices when not in use. These devices draw power even when not actively in use. Smart power strips are now available that can automatically turn off peripherals that are plugged in to the same strip based on the power state of the main device, typically the PC/laptop itself.

Implementing these power saving settings can lead to significant reductions in energy consumption, potentially ranging from a few percent to over 50% in some cases. Give us a call if you need help reviewing your power settings and start conserving energy today.

## Staff PICK Snip & Sketch

Jandy's favorite productivity app is **Snip & Sketch**.

Windows 11 replaced the legacy Snipping Tool and Snip & Sketch apps with a new version that combines the best features of both with an updated interface. It allows you to snip a section of your screen (rectangular, freeform, window or full screen) where you can highlight and/or mark it up, copy to your clipboard to paste into a Teams message or email, or even save it as a picture.

This is a great way to share a screenshot or visually explain changes to a document with a colleague. After all, a picture is worth a thousand words!

Use this keyboard shortcut to capture a quick snip:

⊞ + shift + S

Better yet… pin the app to your Task Bar for easy access!

### Clipboard History

To see what you have recently copied, click the Windows key and V.

(⊞ + V)

Clipboard allows you to paste and pin commonly used items.

### How to Reopen a Tab in Chrome

**For a PC:** Control+Shift+T

**For a Mac:** Command+Shift+T

Or, right click the Chrome icon in task bar, then choose the closed tab under 'Recently Closed'

### Outlook Shortcuts: Create a New Appointment

**Create an appointment from mail view:**
[Ctrl]+[Shift]+Q

**Create an appointment from calendar view:**
[Ctrl]+N

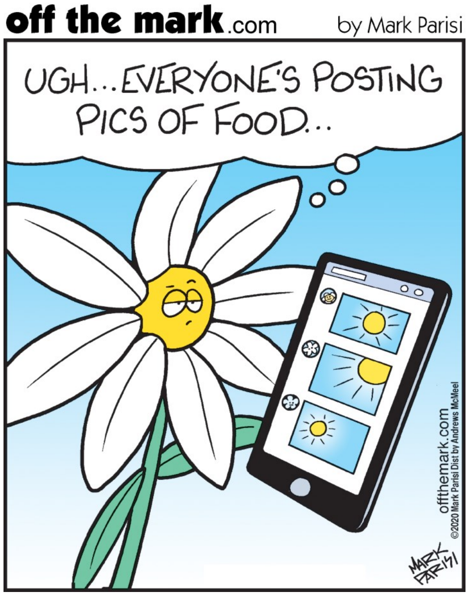
**Create an appointment from any view:**
[Ctrl]+[Shift]+A

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

## Inside This Issue

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

*"What we are doing to the forests of the world is but a mirror reflection of what we are doing to ourselves and to one another."*
— Mahatma Gandhi


off the mark.com
by Mark Parisi
UGH...EVERYONE'S POSTING PICS OF FOOD...
offthemark.com
©2020 Mark Parisi Dist by Andrews McMeel
MARK PARISI

**From the desk of Cathy Coloff**

In 2020, Doug and I had planned to visit Peru and a small part of the Amazon rainforest. Sadly, our trip to Peru has been postponed indefinitely. June 22 is National Rainforest Day—so, in lieu of actually going to Peru, I plan to take advantage of the many wonderful resources online to explore the Amazon rainforests virtually. Did you know that over 50% of our planet's biodiversity is found in rainforests? The rainforests cycle water through their network of trees creating reliable water sources to entire continents. The tree networks and the processes they support serve literally millions of people.

When I think about the Internet and the network of computers it has created and the millions of people it serves, I am always amazed. It's taken years for the processes that the rainforests support to develop and create the balance that our world needs to survive. I hope that our world's computer network, despite its explosive growth, will quickly help us all find ways to live in balance with our wonderful world. In the meantime, I will continue to look for ways to reduce both my and IT Radix's carbon footprint to ensure that the rainforests of the world exist for years to come. I hope you'll join me!

Cathy