



Can You Handle the Truth?

The Importance of Vulnerability Scans for Your Network

In the iconic courtroom scene in *A Few Good Men*, Colonel Jessup's explosive line, "You can't handle the truth!" resonates deeply with the challenges faced by business owners and managers today. The truth about your network's vulnerabilities is something to confront head-on. Ignoring these truths can lead to disastrous consequences, but by embracing regular external and internal vulnerability scans, you can protect your business and ensure its longevity.

The External Threats

External vulnerability scans are like the relentless questioning by Lieutenant Kaffee, probing for weaknesses that could be exploited by external attackers. These identify potential entry points in your network, such as open ports, outdated software, and misconfigured firewalls. By addressing these vulnerabilities, you fortify your defenses against cybercriminals who are constantly seeking easy targets.

A new comprehensive data privacy law, the New Jersey Data Protection Act (NJDP), took effect on January 15, 2025. This law is designed to protect the personal data of NJ residents.

Additionally, many industries have stringent compliance requirements, such as PCI DSS for payment card data security. Regular external scans help you meet these standards, avoiding hefty fines and legal repercussions. Employ these scans to protect your customers' sensitive information.

The Internal Dangers

Just as Colonel Jessup's hidden actions were brought to light, internal vulnerability scans reveal your network's weaknesses. Internal scans scrutinize your internal systems, identifying vulnerabilities that could be exploited by insiders or malware that has bypassed external defenses. From outdated software to misconfigured access controls, internal scans provide a comprehensive view of your network's security posture.

Internal threats, such as disgruntled employees or contractors with access to sensitive information, can be as dangerous as external attackers.

(Continued on page 2)

Take Note

Celebrating Earth Day with Free E-Waste Recycling

Drop off your e-waste at our IT Radix office during the month of April between 10am-4pm.

Acceptable items here: www.it-radix.com/recycling

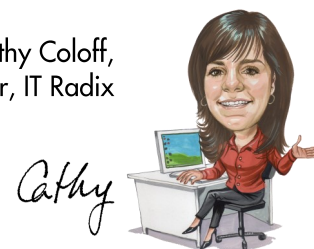
Over the years, our April recycling event has helped properly recycle over 20 tons of e-waste. Let's make 2025 our best collection yet—join us in keeping e-waste out of landfills!

Core Value: Clients Come First

We always do the right thing for our clients, and striving to exceed their expectations is our top priority. But don't take our word for it. See what some of our clients have said about us here:

www.it-radix.com/testimonials

— Cathy Coloff,
Owner, IT Radix



Talk Nerdy to Me



Can You Handle the Truth?

(Continued from page 1)

Conducting internal scans mitigates against these, ensuring your internal defenses are as robust as your external ones.

The Benefits


Embracing the truth about your network's vulnerabilities brings numerous benefits. Enhanced security is the most obvious, as regular scans help you identify and address weaknesses before they can be exploited. This proactive approach can save your company the significant costs of data breaches, including legal fees, fines, and reputation losses.

Likewise, knowing that your network is regularly scanned, and vulnerabilities are addressed provides peace of mind for management and ownership. You can focus on your core business activities, confident that you are protected.

In *A Few Good Men*, the truth was a matter of life and death. In the world of cybersecurity, the truth about your network's vulnerabilities is equally critical. Regular external and internal vulnerability scans should be an integral part of your cybersecurity strategy. They provide a clear and honest assessment of your network's security, allowing you to take the necessary steps to protect your business.

Remember, in the ever-evolving landscape of cybersecurity, the key to staying ahead is to always be prepared and vigilant. Just as Lieutenant Kaffee sought the truth in the courtroom, you must seek the truth in your network's security. Then you can protect your business from the continuous onslaught of daily threats.

Want to know the truth about your networks' vulnerabilities? Give IT Radix a call today to discuss how a set of comprehensive vulnerability scans can give you and your team some peace of mind.



Avoid Using Browser Autofill for Sensitive Info

Disable autofill for passwords, credit card numbers, or other sensitive data in your browser to reduce the risk of unauthorized access. Turning off autofill for sensitive details helps keep your information secure.

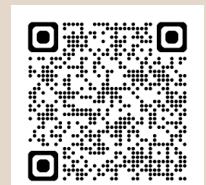
Using a password manager? Most offer secure browser extensions to fill in credentials safely. A little extra caution can go a long way in protecting your personal and financial data!

Stay safe and browse smart!

Microsoft Spotlight: Time to Say Goodbye to Windows 10

Microsoft has set October 14, 2025, as the end-of-life (EOL) date for Windows 10. Operating this software after this date is an open invitation to attackers.

Unlock the future with a free Windows 11 readiness review! Find out what it will take to move from Windows 10 to 11. Don't miss out on this exclusive offer!



www.it-radix.com/win11

Special Offer: Free Windows 11 readiness review!



Just Keep Swimming

The Unsung Heroes of the IT Radix Help Desk

To our clients, the IT Radix Help Desk professionals are the unsung heroes who embody the spirit of "Just Keep Swimming" from the beloved Pixar movie, *Finding Nemo*. Daily, they face a sea of new and recurring challenges, yet they persist with unwavering determination to assist our clients in navigating the digital waters.

Password resets are a daily ritual, akin to Dory's constant forgetfulness. Our staff patiently guides client users through the process, ensuring they regain account access. When faced with slow computers, they channel their inner Marlin, troubleshooting and optimizing systems to restore speed.

Software malfunctions can feel like navigating through a jellyfish forest, but our professionals calmly apply patches and updates to keep applications running smoothly. Trouble connecting remotely is another common issue, reminiscent of Nemo's homeward journey. They provide step-by-step assistance, ensuring clients stay connected and productive.

No matter the challenge, the key is to just keep swimming.

System crashes and the dreaded "blue screen of death" are like the sudden appearance of Bruce, the shark—unexpected and alarming. Here too, our staff dive in fearlessly, diagnosing and resolving hardware and software conflicts to bring systems back to life. Network connectivity issues and wireless problems are tackled with the same persistence ensuring seamless communication and data flow.

Printer problems and login difficulties may seem mundane, but they are a daily occurrence. Our staff approach these issues with the same dedication as Dory's mantra, "Just keep swimming," providing solutions and maintaining the smooth functioning of office equipment.

Through it all, IT Radix professionals demonstrate remarkably positive attitudes combined with grit and resilience. They stay calm and friendly under pressure. Their technical expertise ensures that the digital world of our clients keeps on churning. Like the characters in *Finding Nemo*, they know that no matter how daunting the challenge, the key is to just keep swimming.

Don't Be a Target

(Continued from page 4)

3. **Beware of Unsolicited Offers.** If an email promises a prize, gift, or opportunity that requires personal or payment info, it's likely a scam. If it sounds too good to be true, it probably is.
4. **Be Cautious with Attachments and Links.** Never click links or open attachments from unknown senders. These may contain malware designed to compromise your system. If an email pressures you to act fast, that's a red flag.
5. **Watch for Urgency and Odd Requests.** Scammers create a sense of urgency to make you act without thinking. If an email requests sensitive information in an unusual way, be suspicious.

If you receive a questionable email, reach out to us! We'll help you determine if it's safe. Stay vigilant! Together, we can outsmart cyber-criminals and keep your digital world secure.

Trivia Contest

The first person to send an email to resource@it-radix.com with the correct answer to our trivia question will win a \$50 movie theater gift card!

Q:

"You are named after the dog?" is a quote from which movie?

Inside This Issue

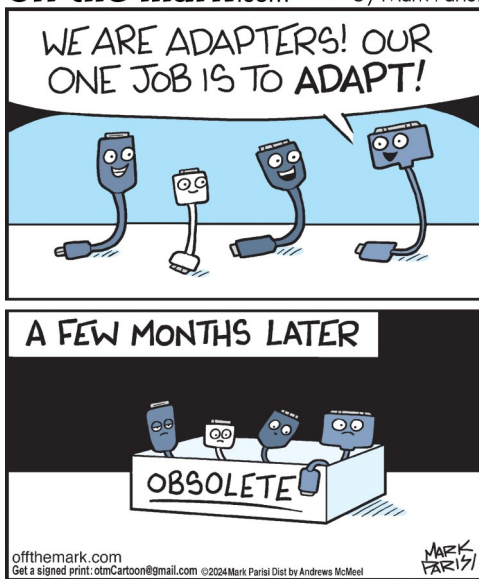
- The truth about your networks' vulnerabilities
- Why you should not use browser autofill for sensitive data
- How to recognize suspicious emails

April 2025

*"Be so good they
can't ignore you."*

— Steve Martin

off the mark.com by Mark Parisi



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

Don't Be a Target



Stay Vigilant Against Suspicious Emails

Have you received a suspicious email lately—maybe asking you to reset your Microsoft 365 password or send money? Cybercriminals are getting smarter in their attempts to trick you.

Remember, they often target people, not just systems. Stay safe by following these tips:

1. **Scrutinize Every Email.** Even if it looks like it's from someone you know, double-check. Hackers often spoof email addresses to appear legitimate.
2. **Check the Sender's Email Address.** Pay attention to subtle changes, like an extra letter or a different domain. If something seems "off," verify with the sender before taking action.

(Continued on page 3)