October 2024

IT Radix Resource

We make IT work for you

Monsters Lurking in the Digital World

"I was working in the lab, late one night" is certainly not what you would expect to be the opening lyrics to a hit song. However, in the fall of 1962, those opening lyrics and more were the rage all over the U.S. as 1-Hit Wonder, Bobby (Boris) Pickett sang "The Monster Mash." Pickett, auditioned for acting jobs by day and sang with a band called The Cordials. One night he did a parody of a current hit song in the voice of Boris Karloff and the audience responded very favorably. That encouraged Pickett and friend Lenny Capizzi to do more with the idea which led to "The Monster Mash." The musicians in this recording were called "The Crypt-Kickers" and included Grammy award winner Leon Russell. And one of the background singers on the track is Darlene Love, famous for the holiday hit, "Christmas (Baby Please Come Home)."

Computer viruses and malware are a bit like monsters that lie in wait in the digital world, waiting to pounce on unsuspecting victims. Sometimes they attack a computer with brute force and sometimes they are allowed in unbeknownst to the PC user/victim. Like these demons, they come in many different forms and can cause all sorts of damage. Some viruses are like vampires, sucking the life out of your computer by slowing it down or deleting important files. Others are like zombies, infecting your computer and turning it into a mindless drone that can be controlled by hackers. Malware can also be like werewolves, changing its form to evade detection by antivirus software.

The most common computer viruses and malware include the following:

- **Boot Sector viruses** are difficult to remove and attack the master boot record, usually spread by USB devices and emails.
- **Polymorphic viruses** are hard to detect and morph every time they replicate making removal arduous.
- **Cavity viruses** attack empty space within codes, not damaging the code, thus are frequently unnoticed.
- **Resident viruses** attached to the computer memory can be removed in part, but not totally if hidden in seldom-used applications.
- **Trojan horse viruses** are masked as legitimate programs. Once installed they have total access.
- **Worm viruses** replicate quickly and can easily damage a computer and slow down a network.
- **Macro viruses** attack Microsoft Office documents and execute vicious code in your system.

(Continued on page 2)

Take Note

October 30
WEBINAR
Tech Talk:
AI Disguises: Deep Fakes
www.it-radix.com/webinar
Starts @ 12:10pm sharp

October is Cybersecurity Awareness Month
Combat cybercrime!
Ask us about our Security Awareness Training and advanced security solutions.

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

Monsters Lurking

(Continued from page 1)

- **Botnets** are malware used to control our computer remotely and send spam emails.
- **Rootkit malware** hides its presence and attempts to steal data.
- **Spyware and Adware** collect information about your web surfing without your knowledge, stealing information, tracking your habits, and displaying undesired content.
- **Ransomware** encrypts your files, damages your machine, and demands payment in exchange for providing a decryption key.

Just like how garlic repels vampires, there are ways to protect your computer from these digital monsters. Installing advanced antivirus endpoint detection and response software and keeping it up to date is like having a cross to ward off vampires or a silver bullet to kill werewolves. So is employing a Zero Trust strategy that allows only approved programs to run on a PC.

Reach out to us at IT Radix to keep your computer safe from the monsters that lurk in the digital world.

Deepfakes Are Coming to the Workplace

Deepfakes use AI and machine-learning to make it seem like someone is saying something they never actually said. This technology, like any other, can be used for good or bad. For instance, David Beckham used AI to speak nine languages in a malaria awareness campaign. Conversely, pornographic deepfakes of Taylor Swift went viral on X, and audio deepfakes of Biden caused concern among experts.

Deepfakes aren't happening only to high-profile politicians and celebrities—they are quickly making their way into the workplace. In April 2023, forensics research company Regula reported that 1/3 of businesses worldwide had already been attacked by deepfake audio (37%) and video (29%) fraud. Regula also noted that the average cost of identity fraud, including deepfakes, for SMBs is $200,000.

How Deepfakes Are Impacting the Workplace

While deepfake technology is used to commit a variety of crimes, there are two ways they currently cause harm to businesses: (1) identity/impersonation fraud schemes, and (2) harm to company reputation.

One of the most common deepfake attacks is when AI impersonates an executive's voice to steal credentials or request money transfers from employees. Other attacks include deepfake videos or audio of a CEO or employee used to disseminate false information online that could negatively affect a brand. More than 40% of businesses have already experienced a deepfake attack, according to authentication experts at ID R&D.

(Continued on page 3)

Service Spotlight: Arm Your Staff With Security Knowledge!

The role of your staff in preventing a cybersecurity event cannot be overstated. Over 85% of breaches involve a human element facilitating a hack, often related to stolen credentials. You can prevent this by helping your employees understand how to avoid the risks of spam, spear phishing, malware, and social engineering. The solution? Provide Security Awareness Training and Testing to minimize your risk.

Special Offer: Sign up for Security Awareness Training in the month of October and get a Baker's Dozen—That's 13 months for the price of 12! *new signups only* (www.it-radix.com/security-awareness-training)

End of Life: The Final Countdown

Some things in life are as steady as the sun rising every morning or the timeless sparkle of diamonds. But, let's be honest, it's hard to come up with many things that truly last forever.

In the ever-evolving landscape of technology, there comes a moment when even the most robust software and hardware must face their twilight hours. Like a sun setting on the digital horizon, these applications reach their End of Life (EOL). It's bittersweet—a crescendo of obsolescence and nostalgia. As we ponder this, we cannot help but hear the haunting lyrics of the band Europe's 1986 hit, "The Final Countdown." Nothing stays the same. Indeed, everything tech related comes with its own expiration date.

Yes, today's software and hardware are born with a "best before" tag. As time marches on, support for these tools eventually winds down, leaving them without crucial updates. This is a bit like leaving a window open for hackers who are always on the lookout for a chance to sneak in. To dodge such unwelcome guests, staying in touch with your vendors or seeking advice from seasoned pros like IT Radix is key—we're here to help you keep those risks at bay.

Managing your tech inventory isn't just about keeping things tidy; it's a cornerstone of cybersecurity and efficiency. Let's dive into why keeping your technology fresh and up to date is a smart move:

- You'll enjoy the latest security enhancements, keeping those pesky hackers at bay.
- Your shiny new software will play nice with your hardware, avoiding any awkward compatibility issues.
- You'll sidestep complex compliance issues that could lead to fines or other serious problems.
- Operating costs can be more predictable, without the surprises that end-of-life (EOL) tech might throw your way.
- Say goodbye to unnecessary downtime, often the side effect of sticking with older software versions.

Consider this: many organizations are still running on Windows 10, which will reach its EOL on October 14, 2025, after a good ten-year run. Past that date, any new security gaps will remain open, leaving those PCs more exposed to attacks. With a year to go, now is the time to start the "final countdown" on your plans to move to Windows 11 or exploring other options.

Feeling a bit overwhelmed? No worries! The team at IT Radix is always here to chat about managing your tech gear effectively, helping you boost productivity while keeping risks to a minimum.

Deepfakes Coming

(Continued from page 2)

What to Do About It

There are a few simple things you can do to prevent deepfakes from having damaging consequences on your business:

1. **Review Technology and Communication Policies**: Ensure transparent communication practices and make sure your team knows how communications are handled internally. Employees should be suspicious of unusual requests for money or information and verify any uncertain email or phone requests.

2. **Incorporate Deepfake Spotting in Cybersecurity Training**: Teach employees how to spot deepfakes, such as unnatural eye blinking, blurry face borders, artificial-looking skin, slow speech, and unusual intonation.

3. **Develop a Response Plan**: Prepare for future deepfake attacks by discussing how to respond if an attack occurs. Although there's no perfect solution yet, being unprepared is the worst scenario.

Be proactive and have a plan to combat deepfakes! IT Radix is here to help. Give us a call to schedule cybersecurity awareness training for your employees today. Check out our special offer on Page 2.

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

"Better to build a bridge than a wall."
— Elton John

From the desk of Cathy Coloff

October is Cybersecurity Awareness Month. At IT Radix, I've had the opportunity to see a wide range of cyber-based incidents and the opportunities for more are vastly expanding. In most cases, a cyber incident starts with a person. Someone is well-meaning, doing their job and just trying to get things done. While we can implement cybersecurity solutions to help reduce and prevent incidents, we cannot prevent a person from falling prey. This is why it is so important to continuously educate, remind, and reinforce layered cybersecurity practices.

I've seen a business owner turn white at the realization that they are going to have to pay hundreds of thousands of dollars to protect their business and their clients when someone at their company inadvertently fell prey to a cyber scam of some type. That feeling in the pit of my stomach as I felt their dismay will never be forgotten.

So, this month, please… educate yourself, your team members, and even your friends and family about the pitfalls of cyberspace, particularly in the security arena, and how to safely use technology to your advantage. Our mission is to help you succeed, but it begins with you.

Have a safe and happy Halloween!