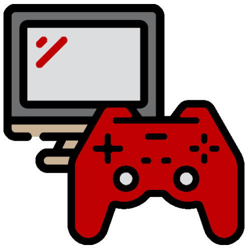
October 2025

IT Radix Resource

We make IT work for you



# Shall We Play a Game?

## *WarGames* Can Teach NJ Businesses About Cybersecurity

In the 1983 techno-thriller *WarGames*, a teenage hacker accidentally accesses a U.S. military supercomputer and nearly launches a global nuclear war—mistaking the system for a game. The film, ahead of its time, captured the rising anxiety about computer security in a networked world. Four decades later, one chilling line still echoes: "Shall we play a game?"

Today, this quote takes on a new meaning—not as a threat, but as a tool. Across industries, including right here in New Jersey, small businesses are starting to "play games" of their own: cybersecurity simulations designed to help IT teams prepare for real-world attacks before they happen.

### Why Simulate Cyberattacks?

October is Cybersecurity Awareness Month—a reminder that threats are constant, evolving, and not limited to large enterprises. Small businesses are increasingly targeted due to often having weaker defenses. According to the 2024 Verizon Data Breach Investigations Report, 61% of small businesses experienced at least one cyber incident in the past 12 months.

Simulations and war games offer a proactive way to build resilience. They allow your internal teams—and your IT partners—to test systems, stress-test protocols, and train people on how to respond when the stakes are high. Think of it like a fire drill, but for cyberwarfare.

### WarGames: More Than a Movie

In *WarGames*, the fictional supercomputer "WOPR" learns from simulations, ultimately realizing that nuclear war is a game no one wins. That's an apt metaphor for modern cybersecurity. Simulations train teams not just how to fight off attacks, but how to think like attackers. The goal isn't to scare, but to learn.

In a typical cybersecurity war game, teams are divided into attackers (Red Team) and defenders (Blue Team). Red tries to breach a system using known exploits or novel tactics. Blue monitors, defends, and responds. Sometimes, a White Team oversees the whole exercise to keep it structured and educational.

*(Continued on page 2)*

## Take Note

**October is Cybersecurity Awareness Month**

Combat cybercrime!
Ask us about our Security Awareness Training and advanced security solutions.

**October 22**
WEBINAR
Tech Talk:
**Unleash the Force:
Harness Microsoft Copilot
AI for Your Success**
www.it-radix.com/webinar
Starts @ 12:10pm sharp

### Did you know...

Microsoft 365 Includes an AI Assistant! Copilot can draft your emails, summarize meetings, and even build PowerPoint decks for you. It's like having a super-smart intern who never takes a coffee break.

— Cathy Coloff,
Owner, IT Radix

Cathy

## Talk Nerdy to Me

## Productivity is a Snap Away

Working on one monitor doesn't mean you have to juggle overlapping windows. Windows Snap Layouts make it easy to organize your screen. Want to compare two documents side by side? Press ⊞ **+ Left or Right arrow** to snap a window to one half of the screen. Snap your window into a corner by adding the **Up or Down arrows**—perfect for multitasking with four apps. Whether you're editing, researching, or just keeping email in view, Snap Layouts help you stay organized and productive without the clutter. Give it a try!

# Shall We Play a Game?

*(Continued from page 1)*

For small businesses without in-house IT staff, trusted Managed IT providers—like IT Radix—can run scaled, customized versions of these simulations. Whether it's a mock phishing attack, a simulated ransomware breach, or a tabletop exercise walking through a crisis scenario, the outcome is the same: your team gets better prepared.

### How Simulations Help New Jersey Businesses

Small businesses across New Jersey—from law and accounting firms in Morristown to manufacturers in Edison—are realizing that cybersecurity isn't just an IT problem. It's a business continuity issue. It affects your data, your reputation, and your ability to operate. Simulations can help:

- **Boost Response Time**. Teams learn how to spot, report, and act on suspicious behavior faster.
- **Reveal Weaknesses**. You'll uncover gaps in your processes, backups, or communication lines.
- **Train Staff**. Everyone from reception to leadership becomes part of the security perimeter.
- **Meet Compliances**. Fulfill insurance and regulatory requirements.

### Let's Not Wait for Reality to Hit

In *WarGames*, it takes a near-catastrophe for people to realize the seriousness of digital threats. Don't let that happen in your business.

October is the perfect time to run a cybersecurity simulation, assess your readiness, and take steps to improve. The investment is minor compared to the cost of a real breach, which now averages over $150,000 for small businesses—and often leads to irreversible damage.

Let IT Radix help you simulate an attack before a real one hits. Because when it comes to cybersecurity, the best defense is preparation—and the best time to start is now. Game on!

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

Users
Devices
Network Traffic
Applications
Data
Zero Trust

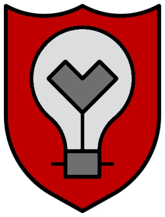
Zero Trust is a security framework requiring all users to be authenticated, authorized, and continuously validated for security configuration *before being granted access to applications and data*. IT Radix's Zero Trust Security Solution:

- ✓ **Zero Day Attacks:** Proactive protection against vulnerabilities
- ✓ **Ransomware:** Ringfencing lets you block any unauthorized use
- ✓ **Per User Limits:** Eliminate the need to grant blanket access
- ✓ **Restrict Applications:** Let only trusted apps access your data

www.it-radix.com/zero-trust

Special Offer: 10% discount on setup of IT Radix's Zero Trust Security Solution through 11/30/25

# More Cybersecurity Tricks Hackers Hate



## Fortify Your Business with These Next-Level (But Still Totally Doable) Cybersecurity Tricks

Let's take your cybersecurity defenses up a notch with more smart ways SMBs can slam the door on cyberthreats. The following three tricks are favorites among IT pros—and hackers can't stand them.

1. **Data Encryption**. Think of encryption as your digital lockbox. It scrambles your data so that even if hackers get their hands on it, they can't read it. It's a must-have for emails, files, and customer records—especially if you're handling sensitive info. Bonus: many cybersecurity insurance policies *require* encryption. The good news? Tools like Google Workspace and Microsoft 365 make this easier than ever. No need for fancy tech skills—just turn it on and keep your data safe.

2. **Limit Employee Access**. Does every employee really need access to everything? Probably not. Giving full access across the board is risky. It increases the chance of someone accidentally (or intentionally) changing something they shouldn't. A better approach? Give each person access only to what they need to do their job. For special projects, temporary access can do the trick. Once the task is done, access goes away. Easy!

3. **Data Backups**. Ransomware attacks are scary—and unfortunately, common. Hackers lock your files and demand payment to unlock them. But if you've got backups in place, you don't have to play that game. Use the 3-2-1 rule: three copies of your data, two types of storage, and one off-site (like the cloud). And don't forget to test those backups. You want to know they'll work *before* you actually need them. IT Radix's managed service plans include a local and off-site backup that is proactively monitored and tested regularly.

Cybersecurity doesn't have to be complicated or expensive. These simple steps make a big impact—and hackers know it. If you haven't implemented them yet, there's no better time than now. Your future self will thank you.

And remember, if you need a hand putting these protections in place or have questions about your cybersecurity, IT Radix is here to help!

# Snackfished? Don't Take the Bait

*(Continued from page 4)*

Is it the end of the world if you get tricked by a fake snack? Definitely not. But it's a helpful reminder to pause before hitting share or hopping in the car to track one down. Just because something *looks* real doesn't mean it is.

The takeaway? Have fun with viral content, but keep a healthy dose of skepticism in your back pocket—especially when snacks are involved!

When it comes to sorting fact from fiction in your tech world, IT Radix is here to help.

Proudly folded & sealed by Central Park School

## Trivia Contest

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

Q:
Which Hollywood actress is also the co-founder of a technology called "Frequency hopping" that laid a key foundation for future communication systems, including GPS, Bluetooth, and Wi-Fi?

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

## Inside This Issue

## October 2025

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

> *"The way I see it, if you want the rainbow, you gotta put up with the rain."*
>
> — Dolly Parton

off the mark.com
by Mark Parisi
THEY SAY SHE NEVER LEAVES THE HOUSE
©2012 Mark Parisi Dist. by Universal UClick for UFS
MARK PARISI
offthemark.com

Permission for IT Radix to use cartoon in print/electronic.

# Are You Being Snackfished?

## Don't Take the Bait:  Even Snacks Can Be Clickbait

If you've ever found yourself searching store shelves for clear ketchup or chocolate-flavored Pringles after seeing them on Instagram… you might've been snackfished.

Snackfishing is a growing trend where influencers post fake—but highly convincing—photos or videos of outrageous food products.  These "products" don't actually exist, but they look real enough to send curious snackers on a wild goose chase.  It's a playful jab at the food industry's habit of releasing bizarre or gimmicky items just to go viral (pickle-flavored soda, anyone?).

While most of these posts are meant as jokes, they're surprisingly effective at fooling people.  That's the point:  snackfishing shows just how easy it is to believe what we see online—especially when it's paired with eye-catching visuals and buzzworthy hashtags.

*(Continued on page 3)*