IT Department October 2025

NewsLetter

Cybersecurity Horror Stories \\ Protecting Yourself \\ dark and stormy night \\ *Remembering* "ILOVEYOU"

🎃 "Cybersecurity Horror Stories: Tales from the Server Room"

This Halloween, we're diving into the dark side of IT with real-life cybersecurity horror stories that remind us why vigilance is key. These tales are not just spooky—they're cautionary lessons for every tech professional and general users of technology.

🧟 The Mother of All Breaches (MOAB)

A staggering 26 billion records were found exposed on an unsecured server in 2024. This mega-leak combined data from LinkedIn, Twitter, Tencent, and more—fueling identity theft and credential-stuffing attacks worldwide.

🧛 The Eternal Haunting – Ticketmaster Breach

Over 560 million customer records were stolen and sold on hacker forums. The breach included order histories, payment info, and personal details—just as the company faced a federal antitrust lawsuit.

🧠 The Glitched Feast – Jollibee Foods Corp

A threat actor leaked 11 million customer records, including birth dates and credit card numbers. The attack exposed serious flaws in the company's data protection practices.

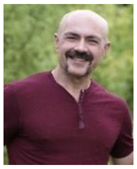
🏨 The Hotel of Horrors – Marriott/Starwood Breach

A breach inherited from Starwood Hotels exposed 500 million guest records over four years. Passport numbers, addresses, and travel histories were compromised—leading to a $123M GDPR fine.

🔥 The SolarWinds Specter

Russian hackers infiltrated the Orion software update, breaching 18,000+ organizations, including Microsoft and U.S. government agencies. This supply chain attack remains one of the most sophisticated in history.

Protecting Yourself in Today's Workplace



Cybersecurity threats have grown in scale and cost over the past decade, affecting not only businesses but also the staff involved. Malware infections have risen nearly 90%, ransomware accounts for over 30 percent of all cyberattacks (with global payments topping $1.1 billion in 2023), and phishing remains the most common threat, with credential theft up more than 700% last year. For businesses, these attacks can mean regulatory penalties, lost revenue, reputational damage, and—most importantly for us—serious HIPAA violations if protected health information (PHI) is exposed. On the personal side, victims face identity theft, empty bank accounts, and long-term recovery challenges.

The warning is clear: protecting your digital life isn't optional. Every device—PC, laptop, phone, or tablet—should run reputable antivirus/antimalware protection and be kept updated. Strong authentication, such as multi-factor (MFA) login, should be used for both business and personal accounts. Be cautious with ALL links, emails, and downloads, especially when accessing sensitive systems; phishing remains the number one way attackers break in. Avoid public Wi-Fi for work unless using a trusted VPN, Bridges Wi-Fi is OK for work. Most importantly, never store or share HIPAA-protected material through unencrypted apps or personal accounts (facebook, gmail, yahoo, chat boards, etc)—only use approved business systems that meet compliance standards. Regular data backups are also essential to recover quickly from ransomware without paying criminals.

By applying these practices in both your Bridges professional work and in your personal life, you help protect not only your own identity and finances but also the other staff and our program participants, and business partners. Business operations depend on you to be safe. Cybersecurity is everyone's responsibility, and a strong personal commitment helps build a safer workplace for all.

HIPAA Best Practices for Staff

- **Use only approved systems**: Never send PHI (Protected Health Information) through personal email, or unencrypted apps.
- **Keep devices protected**: Antivirus software and automatic updates must run on every device used for work.
- **Strong logins only**: Use multi-factor authentication (MFA) and never share your passwords.
- **Be alert for phishing**: If a message looks suspicious, don't click—report it.
- **Work securely on the go**: Use a VPN when on public Wi-Fi, and lock devices when unattended.
- **Control access**: Only access PHI you are authorized to see; never share logins.
- **Back up safely**: Rely on approved business backups, not personal drives or cloud accounts.

Remember: A single slip can cause a HIPAA breach, fines, and loss of trust. Treat PHI as if it were your own most private information.

The unknown drive

It was a dark and stormy night in the IT department. The fluorescent lights flickered overhead, casting long shadows across the rows of humming servers. Most of the office had gone home, but a lone sysadmin named Mike stayed behind, determined to patch one last vulnerability before the weekend.

That's when he found it — a small, unknown flash drive on the break room table. "Found in parking lot", was scrawled on a sticky note. Against their better judgment — and every cybersecurity policy ever written — he let curiosity get the upper hand.

Mike plugged it into his work desktop.

At first, nothing happened. Then the screens around him blinked to life, one by one, showing lines of code, he didn't recognize. His machine froze. The lights dimmed. Somewhere down the hall, a printer shrieked to life, spitting out page after page of wingdings. (Gaining access)

A message appeared on his screen:

"THANK YOU FOR INVITING ME IN."

Mike yanked the drive out — but it was too late. The network had been breached. Phantom processes began executing. Old admin accounts, long deleted, were suddenly active again. The coffee machine started hissing steam like a banshee. The break room Alexa started reciting binary code backward.

By the time the team returned Monday morning, the entire system had been… changed.

Moral of the (Ghost) Story:

- Never plug in unknown devices — especially ones found in parking lots.
- Always educate yourself on phishing and physical device threats.
- And above all… trust your instincts. If it feels haunted, it probably is.

Happy Halloween from the IT department. Stay safe, stay patched, and beware the ghost in the machine.

Knowing what you want and how to get there. Change, it can be **frightening**

Change is a good thing or at least it can be when accepted. We often change a lot of things in our lives and don't even realize that we have done so. For example, the last time you purchased a new/used car, new clothes, new places to eat, even a new last name.

In technology, change happens every day whether we want it or not. Yes, pretty **scary** at times being that often there is no way back to the past. Please don't forget to change your password.

<u>This months IT News Letter is all about the "Scare"</u>

Short Story : There is a **Poltergeist** in my Printer

Early one October Morning, a Saratoga Bridges staff person came in to work only to find paper strewn across the floor below their printer. The pages were scattered like data on a fragmented hard drive**. In case you don't know what that is, just picture a tree in the fall that has all of its' leaves one day, then the next day 75% of the leaves are now on the ground. Each leaf belonged on the tree but who knows where and those leaves no longer serve a purpose, except to fertilize the earth below the tree**.

Let's see, where was I? Oh yes, now I remember.

The pages had only a few odd letters and symbols on each page. What is this new type of language? Is it someone from the other side trying to communicate with them? Is it text message shortened word acronyms that only the younger generation seem to understand? LOL!

The staff person noticed that the printer had flashing lights going on and off , on and off and on the LCD panel, it said "Please Load Paper." The staff person had no idea why or how this mess happened and why the printer was needing more paper. Although it was demanding more paper, it did use the word "Please" and even though it was only 3 words, it was still considered to be a complete sentence. I guess you could say it was an "Imperative Sentence". Nothing like having a printer tell you what to do, am I right? But why, why was the printer asking, <u>No</u>, demanding more paper and why did it make such a mess on the floor? Could it be possessed? Could there be someone there **lurking** in the dark deliberately printing and using up all of their paper and toner on purpose to save on their very own budgeted expenses?

The staff person **submitting** to the demands of the **Demonic possessed Printer**, they loaded more paper into the tray feeding the **Beast** to only have it spit out more of this unrecognizable **scripture**.

Suddenly, the phone rings, It's IT Tech support calling to see how their printer is working before they close the work order. The staff person says "Help, I think my printer is **Possessed!** NOPE! Turns out that one of the IT guys installed the wrong printer drivers and the printer was printing out garbled text, gibberish, or garbage print, **Ghoulish print**.

No IT staff were harmed in the creation of this fiction based short story saga.

I LOVE YOU

Sometimes referred to as Love Bug, the “ILOVEYOU” worm spread through emails in 2000 posing as a love letter attachment. It infected more than 50 million PCs within ten days and wracked up an estimated $15 billion in expenses to remove the worm. Be careful what you click on!!!

WannaCry

Discovered in May 2017, WannaCry is one of the most infamous ransomware strains ever. Like most ransomware, WannaCry was designed to encrypt files on infected computers and demand a ransom from its victims. However, the malware was unique in that it spread rapidly throughout computer networks by exploiting vulnerabilities in outdated Windows operating systems.

Darkside

The **Darkside ransomware-as-a-service** operation emerged in 2020, gaining infamy a year later with the attack on Colonial Pipeline in May 2021.

The attack led to fuel shortages across the southeastern United States. Colonial Pipeline agreed to pay the criminals who carried out the attack 75 bitcoin (around $4.4 million at the time) in return for a decryption key. Even after receiving the key it took several days to fully restore systems.

What can you do about future malware threats?

Considering how dangerous and far-reaching malware can be, having a strong cybersecurity framework is more important than ever. More specifically, you need strong network security controls, antivirus software, and a comprehensive backup system. Furthermore, you should always update your systems and practice good cyber hygiene to prevent malware from infiltrating your systems.

The Old Spooky Days

WEBCAMS

lemon8
FOREST CAM
@pureeriehistory
01:44:12 am 11/30/2010 0139

05:45 PM
22°F
SPYP

HAPPY OCTOBER

Remember when you hear a knock at the door at 2:30am

ITS NOT GOOD

Send comments to: Editor - Phil Ellsworth pellsworth@saratogabridges.org