Newsletter: October 2024

CYBERSECURITY SCARIES

Unpack the cyber threats lurking in the shadows

THIS MONTH'S TOPICS:

Zombie Accounts

Putting inactive accounts to rest

Haunted Devices

Personal devices at work

Scam of the Month:

A case of unauthorized access...

Monthly Cyber News:

October News and Upcoming Dates...

Welcome to this spooky edition of your cybersecurity newsletter! As Cybersecurity Awareness Month comes to a close, we're diving into the eerie side of cybersecurity. Threats like forgotten accounts or unsecured devices could provide easy access points into your organization and put sensitive data at risk.

In this month's newsletter, explore the hidden dangers of zombie accounts—inactive user profiles that, if left unchecked, can provide a backdoor for attackers. We'll also examine the risks posed by using personal devices for work, and how unauthorized access can expose sensitive data.

ZOMBIE ACCOUNTS

Zombie accounts are unused accounts that still have access to your company's systems. These are often forgotten but can be resurrected by cybercriminals to wreak havoc. Treat zombie accounts like the undead—they need to be put to rest before they cause any harm!

BACK TO LIFE

When employees leave the company or change roles, their old accounts may not be deactivated. Hackers take advantage of these accounts because they are easy to exploit without anyone noticing.

Unless regular audits are conducted to catch these zombie accounts, they might not be identified and removed.

BURYING THE UNDEAD

Check the Deactivation Policy: Make sure your company deactivates accounts when employees leave or no longer need access.

Monitor Access Logs: Keep an eye on who's accessing what, so you can spot any unusual activity from zombie accounts. Report any suspicious activity to a supervisor.

31% of employees in the U.S., U.K. and Ireland report having access to a previous employer's software accounts after leaving the organization.

HAUNTED DEVICES

How your personal devices might be haunting your organization

We’ve all got gadgets we use for work, but did you know that if they aren’t properly protected, they could become haunted by cyber threats? Devices like your phone, laptop, or tablet could get infected with malware (malicious programs designed to steal your information) or become entry points for hackers if they aren’t secure.

The Numbers

A recent report found that 83% of companies allow at least some of their employees to bring their own devices to work.

How a Device Becomes Haunted

When you use your phone or laptop for both work and personal purposes, it only magnifies the number of threats and the implications of a cyber incident. If a cybercriminal gains access, they could steal your data or use your device to access the company network.

How to Stop the Haunting

Keep Your Software Updated: Those pop-up reminders to update your device aren’t just annoying—they’re important! Updates often include patches for vulnerabilities that could lead to a breach.

Avoid Public Wi-Fi: Public Wi-Fi can be dangerous, especially if you’re doing anything sensitive, like logging into work accounts. If you have to use it, make sure to connect through a VPN (Virtual Private Network) to protect your data.

Know your organization’s BYOD security policy: Ask your manager or IT team about your company’s Bring Your Own Device (BYOD) Policy. If you are using a personal device, make sure you follow any security policies in place.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using right now. But in this spooky edition, everything is not as it seems...

James sat in his home office, staring at his laptop in disbelief. The project files he'd been working on for weeks had vanished. The files contained sensitive company information. James retraced his steps, trying to figure out what scam he fell for or what tactics cybercriminals used to trick him. He even considered that it might have been an insider threat. One of his colleagues had shown a particular interest in the project...

James scanned his device for any signs of intrusion. His antivirus software showed no suspicious activity. He couldn't remember falling for any potential scams. He was about to give up when he noticed something odd. Muddy paw prints on the keyboard. It hit him — his dogs, Gertie, Ruby, and Luna, had been in the office that morning and he had left his laptop unlocked. A look at the recycle bin on his computer confirmed that it was not a scam after all. His files had been deleted. James restored the files and vowed to lock his devices from now on, even at home.

Did you spot the red flags?

- James should have locked his device when he left it unattended, even though it was in the privacy of his own home.
- James should turn on automated backups so that any permanent deletions, by humans or pets, won't cost him valuable work.

Enable multi-factor authentication (MFA) to add an extra layer of security, making it harder for anyone to gain access even if they do obtain your credentials.

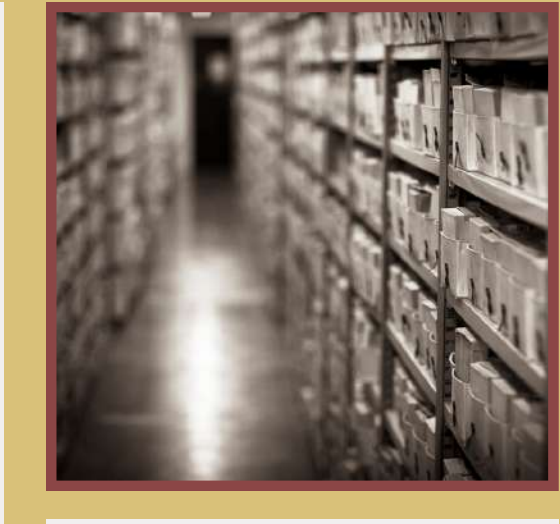
Avoid sharing login credentials or leaving them written down in easily accessible places. Unauthorized access can occur when someone finds your password, either through social engineering or physical access, so it's best to keep credentials private and secure.

CYBER NEWS

OCTOBER 2024

DANGEROUS ONLINE PHARMACY SCAMS ARE CIRCULATING

There have recently been reports of fake online pharmacies selling counterfeit pills such as Oxycodone, Adderall, and Xanax, which may actually contain fentanyl and methamphetamine. Many of these websites appear legitimate, with 24-hour customer support and online reviews. They have vague but legit-sounding names like “Pharmacy Store Online.” These counterfeit drugs pose serious health risks and in some cases are deadly. Consumers should be cautious of unusually low prices and drugs that arrive in broken packaging. Stick to using well-known pharmacies whenever possible.



UPCOMING DATES

November 13th-19th is International Fraud Awareness Week. Make sure to monitor accounts closely for signs of fraud like unexpected charges or changes to your contact information.

INTERNET ARCHIVE BREACH

Internet Archive, the company also behind the Wayback Machine, has recently been hacked. The cybercriminals have allegedly gained access to the data of 33 million users. Some of this data includes images of personal IDs as those wishing to remove records from Internet Archive may have been asked to provide this identifying information. This breach serves as a reminder for all users to use unique passwords on all accounts, and to monitor financial accounts for any signs of unauthorized access.