1991 – 2021 30 YEARS OF EXCELLENCE Computer Technologies, Inc.

TECHNOLOGY TIMES

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

What's Inside

June 2023

Kim Nielsen, CISSP, CCSA
President & Chief Technology Strategist at Computer Technologies Inc.
(248) 362-3800

"As a business owner, you don't have time to waste on technical and operational issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

Do You Know About PII Disclosure Laws in Your Industry?

Whether you work in restaurants or law, healthcare or engineering, you probably use technology to make your day-to-day tasks easier. You make professional connections online, you video chat with coworkers and onboard new customers through our screens. These computer systems thus store data on everything from workflow to employee birthdays to customer credit cards when you sign them up for your services. Whenever personally identifying information, better known in cybersecurity as **PII**, gets transferred through or onto the company database, you as an employee are automatically designated the responsibility for the safety of that information.

It's not only your employer who wants to make sure you keep that information safe. Myriad laws cover the protection of PII in both digital and physical forms that you are subject to, although which ones apply to YOU may change when you start a new job or work with people in different industries.

Laws to Protect National Infrastructure

"Critical infrastructure" refers to those industries that assist our daily lives, from telecommunications to transportation and beyond. Most of the time, people these days book flights, text friends and spend money electronically. That puts all of our information at risk if those databases were to be hacked. That's why governments around the world have created their own data privacy laws, and even joined together to increase our global focus on cybersecurity threats to critical infrastructure and the contractors with whom they work.

- In 2018, the federal government established the Cybersecurity and Infrastructure Security Agency **(CISA)** to oversee the

Continued on pg.2

Continued from pg.1

development of better cybersecurity practices in both the public and private sector.

- The **CCPA** (California Consumer Privacy Act) of 2018 protects the right to know what businesses are doing with collected data.
- **CIRCIA** (Cyber Incident Reporting for Critical Infrastructure Act) was signed in March 2022 and included new cyber-protections, such as mandated reporting within 72 hours of a cyber event and within 24 hours of ransomware payments.

These agencies and laws that have begun popping up in the past few years suggests that the public at large is developing a deeper understanding of how important cybersecurity is to keeping our daily lives on track! The European Union has the **EU General Data Protection Regulation (GDPR)** which has protected the communication, transfer and storage of PII data since it first went into effect in 2018. While the U.S. doesn't have something quite so comprehensive just yet, state and federal governments have clearly been turning their eyes in that direction.

Role-Based Laws

Depending on where you work, you might also be liable for data privacy because of the specific industry you're in. For example, you might be aware of **HIPAA** which protects your medical information from disclosure without your express permission. ALL healthcare providers are beholden to this. Although that's one of the more well-known, did you know that attorneys, bankers and internet providers (to name just a few) have to follow special privacy laws too?

> **When PII gets transferred through or onto the company database, you as an employee are designated the responsibility for the safety of that information.**

You might also be expected to meet various compliance regulations based on the role you play within your organization. For example, an assistant might be responsible for only their machine, but the manager would be additionally responsible for the assistant's compliance to departmental standards. Similarly, the financial department is more vulnerable to certain attacks while the CEO might face other kinds of phishing scams. When you accept a position that handles, transports or stores people's private data, you are automatically beholden to data privacy and compliance laws congruent with the role. Pay attention at your security awareness trainings to learn what's expected of you!

Conclusion

The more people learn about data collection and sales, cybercriminal threats to their digital transactions, and vulnerabilities in their online accounts, the more state and federal governments have been enacting laws to protect PII from inappropriate disclosure. This effort goes back to the '90s, when medical records went digital and the need for electronic protection quickly arose, ultimately spawning HIPAA. In the unending war against unauthorized access to confidential data, we are all responsible for keeping PII safe in communication and when being stored.

Navigating the cyber-landscape safely can be daunting alone. Keep this article in your pack of tips and news about information security!

Free Cyber Risk Audit Will Reveal Where Your Computer Network Is Exposed And How To Protect Your Company Now

At no cost or obligation, our highly skilled team of IT pros will come to your office and conduct a comprehensive cyber risk audit to uncover any loopholes that may exist in your company's IT security.

After the audit is done, we'll prepare a customized "Report Of Findings" that will reveal specific vulnerabilities and provide a Prioritized Action Plan for getting these risk problems addressed fast. This report and action plan should be a real eye-opener for you, since almost all of the businesses we've done this for discover they are exposed to various threats in a number of areas.

Claim Your FREE Assessment Today At:
https://www.cti-mi.com/cyber-security-audit-623/
Or Call Our Office At: 248-362-3800

Security Corner

The Inside Scoop On Insider Threats

We bet that you're a good, hardworking individual who doesn't want to cause problems for your company. You wouldn't *intentionally* leak important information that would compromise the organization in anyway!

Unfortunately, it happens all of the time. They are called **insider threats**.

What Counts as an Insider Threat?

Insider threats can come from employees, contractors or even vendors who have access to confidential information and systems.

The best defense against insider threats is a comprehensive cybersecurity strategy that includes robust authentication measures, regular monitoring of user activity and proactive risk assessment.

Why Should You Be Concerned?

More than one-third of businesses are negatively impacted by insider threats *every year.* Remember, these can be on purpose or unintentional! Some of the most common mistakes insiders make include…

- Sharing your password, or using a weak one
- Not enforcing privileged access controls
- Failure to use multi-factor authentication

Insider threats are a major concern for businesses and organizations when it comes to cybersecurity. Insider threats are responsible for ***60% of data breaches*** to companies like yours.

For more information about Insider Threats and other cyber threats, call us at 248-362-3800 or visit: https://bit.ly/3pilwFF

Is It Time To Ditch Passwords For More Secure Passkeys?

Passwords are the most used method of authentication, but they are also one of the weakest. Passwords are often easy to guess or steal. Also, many people use the same password across several accounts. This practice makes them vulnerable to cyber-attacks.

61% of all data breaches involve stolen or hacked login credentials.

In recent years a better solution has emerged – passkeys. Passkeys are more secure than passwords. They also provide a more convenient way of logging into your accounts.

What is Passkey Authentication?

Passkeys work by generating a unique code for each login attempt. This code is then validated by the server. This code is created using a combination of information about the user and the device they are using to log in.

You can think of passkeys as a digital credential. A passkey allows someone to authenticate in a web service or a cloud-based account. There is no need to enter a username and password.

This authentication technology leverages Web Authentication (WebAuthn). This is a core component of FIDO2, an authentication protocol. Instead of using a unique password, it uses public-key cryptography for user verification.

The user's device stores the authentication key. This can be a computer, mobile device, or security key device. It is then used by sites that have passkeys enabled to log the user in.

Advantages of Using Passkeys Instead of Passwords

More Secure
One advantage of passkeys is that they are more secure than passwords. By default, Passkeys are more difficult to hack. This is true especially if the key generates from a combination of both biometric and device data.

Biometric data can include things like facial recognition or fingerprint scans. Device information can include things like the device's MAC address or location. This makes it harder for hackers to gain access to your accounts.

More Convenient

Another advantage of passkeys over passwords is that they are more convenient. With password authentication, users often must remember many complex passwords at one time. This can be difficult and time-consuming.

Forgetting passwords is common and doing a reset can slow an employee down. Each time a person has to reset their password, it takes an average of three minutes and 46 seconds.

Passkeys erase this problem by providing a single code. You can use that same code across all your accounts. This makes it much easier to log in to your accounts. It also reduces the likelihood of forgetting or misplacing your password.

Phishing-Resistant

Credential phishing scams are prevalent. Scammers send emails that tell a user something is wrong with their account.

They click on a link that takes them to a disguised login page created to steal their username and password.

When a user is authenticating with a passkey instead, this won't work on them. Even if a hacker had a user's password, it wouldn't matter. They would need the device passkey authentication to breach the account.

How To Use ChatGPT At Your Business Responsibly

ChatGPT has revolutionized the way businesses interact with their customers. It has also affected how they get things done.

Teams are using it for everything from emails to generating ideas for product names.

The tool's personalized and informative responses in real-time definitely draw you in. But integrating ChatGPT into your business requires careful consideration.

You want to ensure that things don't get out of hand with employees using the tool irresponsibly.

- Define ChatGPT's Role
- Consider Customer Privacy
- Ensure Human Oversight
- Integrate ChatGPT Into Your Existing Customer Service
- Be Transparent About Using It

What Is Push-Bombing & How You Can Prevent It?

Cloud account takeover has become a major problem for organizations. Between 2019 and 2021, account takeover (ATO) rose by 307%.
Many organizations use multi-factor authentication (MFA) as a way to stop fraudulent sign-ins. But its effectiveness has spurred workarounds by hackers. One of these is push-bombing.

How Does Push-Bombing Work?

When a user enables MFA on an account, they typically receive a code or prompt of some type.

"Hold it! That's not what they mean by 'reboot'."

CartoonStock.com

The user enters their login credentials. Then the system sends an authorization request to complete their login.

With push-bombing, hackers start with the user's credentials and take advantage of that push notification process. They attempt to log in many times. This sends the legitimate user several push notifications, one after the other. When someone is bombarded with these requests, it can be easy for them to mistakenly click to approve access.

Push-bombing is a form of social engineering attack designed to:

- Confuse the user
- Wear the user down
- Trick the user into approving the MFA request to give the hacker access

Ways to Combat Push-Bombing at Your Organization

- Educate Employees
- Reduce Business App "Sprawl"
- Adopt Phishing-Resistant MFA Solutions
- Enforce Strong Password Policies