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

February 2026

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!"

Doxxing: What You Need to Know About This Cyber-Threat

A massive part of maintaining online data privacy is keeping your personal information, like your home address and SSN, off the web. So what happens when a cyberattack specifically aims to uncover and publish your personally identifiable information (better known as PII)?

It's called doxxing, and approximately 11M Americans have been victims of it. Sound scary? Let's dive into more about this threat and how to handle it.

What Is Doxxing?

This cybercrime is particularly dangerous because, although it occurs online, it can have serious real-world consequences for the unfortunate targets. Doxxing occurs when a bad actor publicly posts private, personal, or identifying information about an individual without their consent.

The type of information might include: Full name, home address, phone numbers, email addresses, workplace or employer details, Social Security numbers, and private photos or documents.

Anyone who sees that information can use it to harass, intimidate, and/or threaten the victim… online or in person. Do you want your biggest enemy to see details about your personal life? Probably not!

Doxxing High-Profile Individuals

In recent years, corporate executives at major companies have increasingly become targets of doxxing, especially when their decisions spark public or internal controversy. One common scenario involves a company implementing a return-to-office policy after a period of remote work. If a high-ranking executive

Continued on pg.2

Continued from pg.1

publicly supports this change, it can trigger backlash from employees or online communities who feel strongly about remote work.

In such a case, the executive's personal information (including their home address, phone number, and family details) end up online through platforms like Reddit, 4chan, or social media. The threat actor exposing this information often accompanies the leak with calls to harass the individual or even organize protests near their home. While political figures have been common targets in the past, more and more threat actors direct these attacks at corporate leaders as well.

Staying Safe

As doxxing becomes more common and more dangerous, it can lead to cyberattacks, reputational damage, and real-world threats to physical safety. Once someone puts your information online, you also never know who else has saved it.

The best way to avoid doxxing? Avoid oversharing on social media. That includes your full name, birthday, address, school, or workplace. Set your profiles to private and review your followers or friends list regularly. Remember that your posts have an audience. If you wouldn't share it with your distant acquaintance, then they shouldn't read about it online.

Did you know that your pictures might include metadata that exposes when and where the photo was taken? Posting a lot of pictures can tell determined threat actors where you hang out, go out and work.

Some tricks for staying safe:

- Enable multi-factor authentication (2FA/MFA) on all accounts.
- Use unique, strong passwords with a password manager.
- Avoid using your real name or primary email for public forums, like your gaming platforms and social media

If you find out that you've been doxxed, document everything and report the incident to the platform where your data was published. You might also involve law enforcement if physical threats to your safety arise.

Conclusion

Many places have made doxxing illegal, especially if it involves threats, stalking, or the release of any information that leads to harm.

Doxxing has become a popular form of semi-anonymous retaliation, and we all need to be aware of the dangers of posting too much online.

Security Corner

What Are Insider Threats?

When people hear the term insider threat, they often imagine a disgruntled employee deliberately trying to harm their company. While that can happen, the reality is much harder to detect and avoid.

An insider threat encompasses any security risk that comes from someone who already has legitimate access to systems, data, or facilities. That includes employees, contractors, vendors, and even temporary staff members.

Accidental Insider Threats: The Most Common Kind-When someone unintentionally exposes data or systems, it's still considered an insider threat. Think of any time you've sent a file to the wrong recipient, uploaded documents to a personal cloud account, or reused passwords again and again.

Intentional Insider Threats: When Authorized Users Abuse Access- Intentional insider threats are less common, but much more damaging. These occur when someone knowingly misuses their access, whether for financial gain, revenge, or pressure from outside attackers. Some common examples include: Stealing data before leaving a job, selling credentials, deliberately weakening security controls, or sending private data to outside collaborators

Conclusion
Insider threats may come from intentional cybersecurity breaches inside the organization…but more often, they happen because somebody with legitimate access makes a mistake. If you see strange or risky behavior from a coworker, don't be afraid to say something.

For more information about this topic, call us at 248-362-3800 or visit: https://tinyurl.com/mrxxbw44

The MFA Level-Up: Why SMS Codes Are No Longer Enough (And What To Use Instead)

For years, enabling Multi-Factor Authentication (MFA) has been a cornerstone of account and device security. While MFA remains essential, the threat landscape has evolved, making some older methods less effective.

The most common form of MFA, four- or six-digit codes sent via SMS, is convenient and familiar, and it's certainly better than relying on passwords alone. However, SMS is an outdated technology, and cybercriminals have developed reliable ways to bypass it. For organizations handling sensitive data, SMS-based MFA is no longer sufficient. It's time to adopt the next generation of phishing-resistant MFA to stay ahead of today's attackers.

Why Phishing-Resistant MFA Is the New Gold Standard

To prevent these attacks, it's essential to remove the human element from authentication by using phishing-resistant MFA. This approach relies on secure cryptographic protocols that tie login attempts to specific domains.

One of the more prominent standards used for such authentication is Fast Identity Online 2 (FIDO2) open standard, that uses passkeys created using public key cryptography linking a specific device to a domain. Even if a user is tricked into clicking a phishing link, their authenticator application will not release the credentials because the domain does not match the specific record.

Implementing Hardware Security Keys

Hardware security keys are physical devices resembling a USB drive, which can be plugged into computer or tapped against a mobile device. You simply insert the key into the computer or touch a button, and the key performs a cryptographic handshake with the service. This method is quite secure since there are no codes to type, and attackers can't steal your key over the internet. Unless they physically steal the key from you, there is no way for them to access your account.

Mobile Authentication Apps and Push Notifications

If physical keys are not feasible, mobile authenticator apps such as Microsoft or Google Authenticator are a step up from SMS MFA. These apps generate codes locally on the device, eliminating the risk of SIM swapping or SMS interception since the codes are not sent over a cellular network.

There are still risks. For example, attackers may flood a user's phone with repeated login approval requests, causing a frustrated or confused user to "approve" just to stop the notifications. Modern authenticator apps address this with "number matching," requiring the user to enter a number shown on their login screen into the app. This ensures the person is physically present at their computer before granting access.

Passkeys: The Future of Authentication

Modern systems are embracing passkeys, digital credentials stored on a device and protected by biometrics. Passkeys are phishing-resistant and can be synchronized across your ecosystem, such as iCloud Keychain or Google Password Manager. They offer the security of a hardware key with the convenience of a device that you already carry.

A Simple 15-Minute Daily Cloud Checkup Routine

1. Review Access Logs – Look for logins from unusual locations or at strange times.

2. Check for Storage Permissions – Review the permission settings on your storage buckets and ensure that your private data remains private.

3. Monitor for Resource Spikes – Check for any unexpected spikes in computing power and compare each day's metrics.

4. Examine Security Alerts and Notifications – These often contain critical information about vulnerabilities.

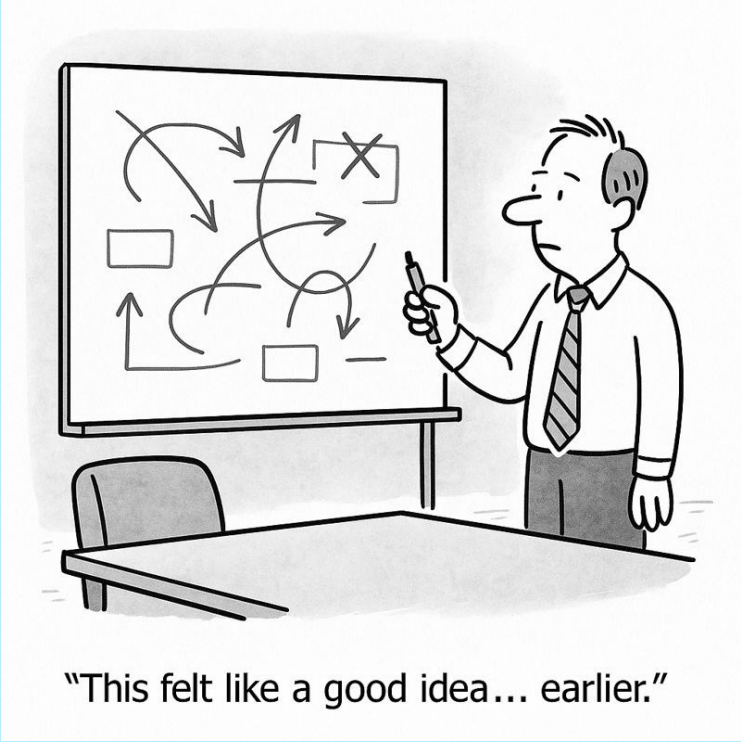
5. Verify Backup Integrity – Check the status of your overnight backup jobs.

6. Keep Software Patched and Updated – Make sure automated patching schedules are running correctly.

The Smarter Way To Vet Your SaaS Integrations

Here are some smart and systematic SaaS evaluation processes that protect your business from third-party risk.

- Scrutinize the SaaS's Security Posture: Your first steps should be examining their certifications and, in particular, asking them about the SOC 2 Type II report.
- Chart the Tool's Data Access and Flow: You need to understand what data the integration will touch by asking a simple, direct question: What access permissions does this app require?
- Examine Their Compliance and Legal Agreements: Carefully review their terms of service, compliance, privacy policies, and how data is stored.



Policies For Employees Working From Cafes And Co-Working Spaces

- Mandate VPN Usage: Employees must use VPN to encrypt all data and establish a secure tunnel over public Wi-Fi.
- Prevent Visual Hacking: Issue and require the use of privacy screens to prevent passersby from glancing and stealing sensitive information.
- Maintain Physical Security: Employees must keep their laptops and devices with them at all times.
- Avoid Confidential Conversations: Employees should not discuss sensitive business matters in public.
- Create a Clear, Written Policy: Publish a comprehensive remote work policy and set a regular review cadence.