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

Malware-as-a-Service Is Using Microsoft Teams to Launch Attacks .....Page 1

FREE Executive Guide: Protect Your Data & Preserve Your Network .....Page 2

Security Corner: Vishing Scams Are On the Rise .....Page 3

Implement Zero Trust For Your Guest Wi-Fi Network .....Page 3

How To Prevent Leaking Private Data Through Public AI Tools .....Page 4

3 Steps To A Formal IT Asset Disposition Policy.....Page 4

January 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!"

Malware-as-a-Service Is Using Microsoft Teams to Launch Attacks

Microsoft Teams has become a staple in modern workplaces, helping employees communicate and collaborate more efficiently. Do you use it to communicate with your coworkers? Send files quickly to other departments? Schedule meetings that will remind you before they happen?

All over the world, over 320M people use Teams. While the platform may feel like a safe, internal environment, hackers have found ways to exploit that trust. Unfortunately, some threat actors have started using it as a launchpad for sophisticated social engineering attacks that unleash malware-as-a-service.

So, what are social engineering and MaaS, and how are these threat actors propagating them through Microsoft software? Let's dive in!

How the Attacks Are Happening

In a recent tidal wave of cyberattacks, threat actors impersonate IT helpdesk personnel during external Microsoft Teams calls. Once on a call, they then employ classic social engineering tactics to convince the victim to launch Microsoft's Quick Assist tool, a legitimate remote support utility.

From there, they walk the employee through running a script that appears to contain a harmless update…but which really installs malware on the machine. Because this method sidesteps traditional email-based phishing filters, it can catch even cautious users off guard!

The malware they're installing is called Matanbuchus; a dangerous type of malware-as-a-service. Think of MaaS like a subscription to cybercrime: attackers pay to

Continued on pg.2

Continued from pg.1

access powerful malware tools that can be customized and deployed without needing deep technical skills.

The Matanbuchus Payload
In this case, attackers used MaaS to drop a "payload." This refers to the part of the malware that performs the real damage.

Once installed, this malware can steal data, open backdoors, or lay the groundwork for even more destructive attacks (like ransomware). Like MaaS, threat actors can also purchase packaged ransomware on the Dark Web.

What You Can Do to Stay Safe
Unfortunately, no single "patch" can prevent this kind of attack. Malware-as-a-service is sold on the Dark Web, making it difficult to shut down. Social engineering tactics meanwhile use increasingly smart methods to avoid detection, not exploiting a traditional software flaw, but rather going after human trust and behavior.

That means defense requires a layered approach:

- Pay attention to your awareness trainings, especially phishing courses that teach you how to recognize fake IT support calls and the dangers of blindly following instructions from unknown contacts (even on familiar platforms like Teams).
- Restrict or monitor your external Teams communications. Your organization may already limit who can contact you from outside the company.
- Be careful who is contacting you via remote access technology.
- Keep systems updated to ensure you're not vulnerable to known exploits.

The more you understand about how phishing happens and best practices to recognize it, the more effectively you can spot, avoid and report these bad actors!

Conclusion
This attack epitomizes why cybersecurity is no longer just about firewalls and software updates; it's about people. Tools like Microsoft Teams are invaluable for collaboration, but they can also be exploited if you don't think critically and act cautiously when you receive a suspicious message.

Phishing remains one of the most prevalent threats to users everywhere. Stay aware, stay cautious, and continue enjoying everything that these collaborative platforms have to offer—without sacrificing cybersecurity.

Security Corner

Vishing Scams Are On the Rise
When people think of cyberattacks, they often picture malware, phishing emails, or ransomware. Sometimes, though, attackers don't need code to compromise an organization; they just need a convincing voice.

Voice phishing, or vishing, has been skyrocketing in the past two years, with a 170% rise in deepfake vishing in the latter half of 2025.

AI clones real voice audio to create a "deepfake," which is a very good copy of someone's speech patterns. Synthetic voices can impersonate your colleagues, managers, or IT staff with chilling accuracy.

Why Vishing Works
Unlike email phishing, vishing exploits tone, trust, and urgency. Attackers often pose as technology support staff, calling under the guise of "resolving" digital issues or reconnecting services. Once they establish rapport, they can bypass your MFA, trick people into granting access, or reset user credentials. All of this gives them full control over your sensitive accounts.

Traditional defenses like spam filters don't work here, because they're convincing you to give them legitimate access to your data.

Protecting Yourself from Vishing
When you get a call that begs you to take immediate action, then is the perfect time to slow down and reassess the situation. Because of spoofing technology, cybercriminals can "clone" their phone number so it appears to come from a trusted number. Always validate who you're speaking to and confirm through a trusted internal channel, not caller ID.

For more information about this topic, call us at 248-362-3800 or visit: https://tinyurl.com/y3skuswv

Implement Zero Trust For Your Guest Wi-Fi Network

Guest Wi-Fi is a convenience your visitors expect and a hallmark of good customer service. But it's also one of the riskiest points in your network. A shared password that's been passed around for years offers virtually no protection, and a single compromised guest device can become a gateway for attacks on your entire business. That's why adopting a Zero Trust approach for your guest Wi-Fi is essential.

The core principle of Zero Trust is simple but powerful: never trust, always verify. No device or user gains automatic trust just because they're on your guest network. Here are some practical steps to create a secure and professional guest Wi-Fi environment.

Build a Totally Isolated Guest Network
The first and most crucial step is complete separation. Your guest network should never mix with your business traffic. This can be achieved through strict network segmentation by setting up a dedicated Virtual Local Area Network (VLAN) for guests. This guest VLAN should run on its own unique IP range, entirely isolated from your corporate systems.

Then, configure your firewall with explicit rules that block all communication attempts from the guest VLAN to your primary corporate VLAN. This strategic containment ensures that if a guest device is infected with malware, it cannot pivot laterally to attack your servers, file shares, or sensitive data.

Implement a Professional Captive Portal
Get rid of the static password immediately. A fixed code is easily shared, impossible to track, and a hassle to revoke for just one person. Instead, implement a professional captive portal, like the branded splash page you encounter when connecting to WiFi at a hotel or conference. This portal serves as the front door to your Guest Wi-Fi.

You can configure it securely in several ways. For example, a receptionist could generate a unique login code that expires in 8 or 24 hours, or visitors could provide their name and email to receive access. For even stronger security, a one-time password sent via SMS can be used. Each of these methods enforces the 'never trust' principle.

Enforce Policies via Network Access Control
Having a captive portal is a great start, but to achieve true guest network security, you need more powerful enforcement, and that is where a Network Access Control (NAC) solution comes into play. NAC acts like a bouncer for your network, checking every device before it is allowed to join, and you can integrate it within your captive portal for a seamless yet secure experience. If the guest's device fails posture checks, the NAC can redirect it to a walled garden with links to download patch updates or simply block access.

Apply Strict Access Time and Bandwidth Limits
Trust isn't just about determining who is reliable, it's about controlling how long they have access and what they can do on your network. Use your NAC or firewall to enforce strict session timeouts, requiring users to reauthenticate after a set period, such as every 12 hours.

Similarly, implement bandwidth throttling on the guest network. It is also a good business practice to prevent network congestion by activities that do not align with your business operations.

Create a Secure and Welcoming Experience
Implementing a Zero Trust guest Wi-Fi network is no longer an advanced feature reserved for large enterprises, but for all business sizes.

How To Prevent Leaking Private Data Through Public AI Tools

Most public AI tools use the data you provide to train and improve their models. This means every prompt entered into ChatGPT or Gemini could be part of their training data. A single mistake by an employee could expose client information, proprietary code and processes. As a business owner, it's essential to prevent data leakage before it turns into a serious liability.

Establish a Clear AI Security Policy

Your first line of defense is a formal policy that clearly outlines how public AI tools should be used. This policy must define what counts as confidential information and specify which data should never be entered into a public AI model, such as social security numbers, financial records, or product roadmaps.

Implement Data Loss Prevention Solutions with AI Prompt Protection

You can prevent leakage of personal information by implementing data loss prevention (DLP) solutions that stop data leakage at the source. Cloudflare DLP and Microsoft Purview offer advanced browser-level context analysis, scanning prompts and file uploads in real time before ever reaching the AI platform.

Conduct Continuous Employee Training

Conduct interactive workshops where employees practice crafting safe and effective prompts using real-world scenarios from their daily tasks. This hands-on training enables them to de-identify sensitive data, turning staff into active participants in data security while still leveraging AI for efficiency.

3 Steps To A Formal IT Asset Disposition Policy

You can't protect what you don't plan for. Start with a straightforward IT Asset Disposition (ITAD) policy that clearly outlines the steps and responsibilities. Simply put, ITAD is the secure, ethical, and fully documented way to retire your IT hardware.

At a minimum, it should cover:

- The process for retiring company-owned IT assets.
- Who does what; who initiates, approves, and handles each device.
- Standards for data destruction and final reporting.

A clear policy keeps every ITAD process consistent and accountable through a defined chain of custody. It turns what could be a one-off task into a structured, secure routine, helping your business maintain a strong security posture all the way to the end of the technology lifecycle.