FEBRUARY
2026

TECH TALK
MONTHLY

THE "DEEPFAKE CEO" SCAM

More in this edition:

MANAGEPOINT

manage-point.com

(414) 485-6169

dsteger@manage-point.com

What's Inside

Dear Fellow Business Owner 👋

There's a new sophisticated evolution in cybercrime that is targeting businesses like yours: the **Deepfake CEO Scam.**

For years, scammers relied on deceptive emails to trick employees into transferring funds. Today, criminals are using Artificial Intelligence to take this fraud to the next level. By harvesting short audio clips from company webinars, social media, or voicemail greetings, scammers can now clone an executive's voice with terrifying accuracy.

The scam typically works like this: An employee in finance or HR receives an urgent phone call or voicemail from what sounds exactly like their CEO or CFO. The "executive" claims they are in a meeting or traveling and demands an immediate, confidential wire transfer. Because the voice sounds authentic and the request is urgent, well-meaning employees often bypass standard security checks.

How can you protect your organization?

The most effective defense is a "verify first" policy. If you receive an unexpected financial request, legitimate executives will not mind if you hang up and call them back on a known internal number. We also recommend establishing a verbal "challenge password" or "safe word" for authorizing sensitive transactions that cannot be spoofed by AI.

If you need assistance updating your verification protocols or training your staff to recognize these advanced threats, we are here to help. Please reach out to us today at email@yourcompany.com to secure your business communications.

David Steger
Owner, ManagePoint

DID YOU KNOW ?

Did you know that, As of May 2019, more than 500 hours of video were uploaded to YouTube every minute. This equates to approximately 30,000 hours of newly uploaded content per hour.

GET IN TOUCH

(414) 485-6169

manage-point.com

dsteger@manage-point.com

THE “DEEPFAKE CEO” SCAM: WHY VOICE CLONING IS THE NEXT CYBER THREAT

The phone rings, and it’s your boss. The voice is unmistakable; with the same flow and tone you’ve come to expect. They’re asking for a favor: an urgent wire transfer to lock in a new vendor contract, or sensitive client information that’s strictly confidential. Everything about the call feels normal, and your trust kicks in immediately. It’s hard to say no to your boss, and so you begin to act.

What if this isn’t really your boss on the other end? What if every inflection, every word you think you recognize has been perfectly mimicked by a cybercriminal? In seconds, a routine call could turn into a costly mistake; money gone, data compromised, and consequences that ripple far beyond the office.

What was once the stuff of science fiction is now a real threat for businesses. Cybercriminals have moved beyond poorly written phishing emails to sophisticated AI voice cloning scams, signaling a new and alarming evolution in corporate fraud.

How AI Voice Cloning Scams Are Changing the Threat Landscape.

HOW AI VOICE CLONING SCAMS ARE CHANGING THE THREAT LANDSCAPE

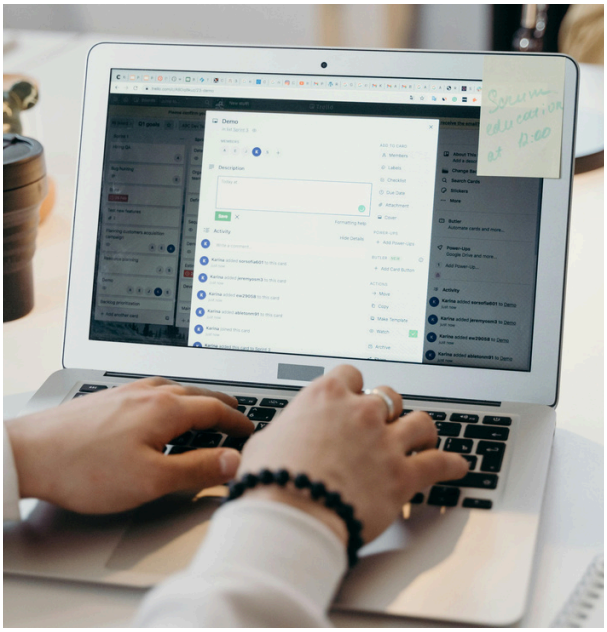
We have spent years learning how to spot suspicious emails by looking for misspelled domains, odd grammar, and unsolicited attachments. Yet we haven’t trained our ears to question the voices of people we know, and that’s exactly what AI voice cloning scams exploit.

Attackers only need a few seconds of audio to replicate a person’s voice, and they can easily acquire this from press releases, news interviews, presentations, and social media posts. A scammer doesn’t need to be a programming expert to impersonate your CEO, they only need a recording and a script.

THE EVOLUTION OF BUSINESS EMAIL COMPROMISE

Traditionally, business email compromise (BEC) involved compromising a legitimate email account through techniques like phishing and spoofing a domain to trick employees into sending money or confidential information. BEC scams relied heavily on text-based deception, which could be easily countered using email and spam filters. While these attacks are still prevalent, they are becoming harder to pull off as email filters improve.

Voice cloning, however, lowers your guard by adding a touch of urgency and trust that



emails cannot match. “Vishing” (voice phishing) uses AI voice cloning to bypass the various technical safeguards built around email and even voice-based verification systems. Attackers target the human element directly by creating high-pressure situations where the victim feels they must act fast to save the day.

CHALLENGES IN AUDIO DEEPFAKE DETECTION

Few tools currently exist for real-time audio deepfake detection, and human ears are unreliable, as the brain often fills in gaps to make sense of what we hear. That said, there are some common tell-tale signs, such as the voice sounding slightly robotic or having digital artifacts when saying complex words. Other subtle signs you can listen for include unnatural breathing patterns, weird background noise, or personal cues such as how a particular person greets you.

SECURING YOUR ORGANIZATION AGAINST SYNTHETIC THREATS

As AI tools become multimodal, we will likely see real-time video deepfakes joining these voice scams, and you will need to know how to prove that a recording is false to the press and public. Waiting until an incident occurs means you will already be too late.

Does your organization have the right protocols to stop a deepfake attack? Contact us today to assess your vulnerabilities and secure your communications against the next generation of fraud.

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.

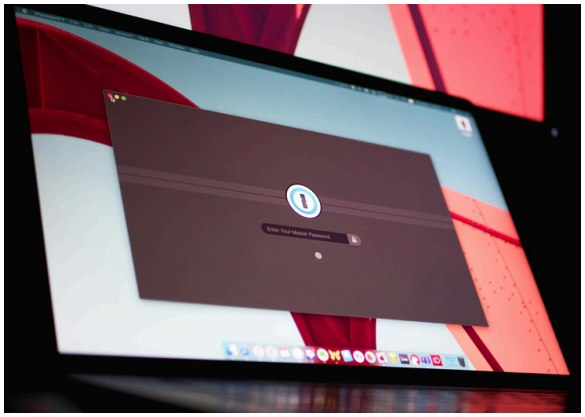
One of the more prominent standards used for such authentication is Fast Identity Online2 (FIDO2) open standard, that uses passkeys created using public key cryptography linking a specific device to a domain. Even if a user is tricked into clicking a phishing link, their authenticator application will 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, they cannot 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.

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.

WHY WINDOWS SERVER 2016'S END OF SUPPORT SHOULD DRIVE YOUR CLOUD MIGRATION PLAN

Time moves fast in the world of technology, and operating systems that once felt cutting-edge are becoming obsolete. With Microsoft having set the deadline for Windows Server 2016 End of Support to January 12, 2027, the clock is ticking for businesses that use this operating system.

Understanding the Security Implications

When support ends, the protection provided by security updates and patches disappears, as Microsoft will no longer fix bugs or vulnerabilities. Hackers often target unsupported systems, knowing any new exploits will go unpatched and open the door to attacks.

Legacy systems put IT administrators in a tough spot. Without vendor support, defending against threats becomes nearly impossible, compliance with industry regulations is compromised, and running unsupported software can lead to failed audits.

The Cost of Doing Nothing

Ignoring the end of support deadline is not a viable strategy. Some businesses hope to delay until the last minute and then rush a migration, but this is extremely risky. Cybercriminals constantly target outdated, vulnerable systems, often using automated bots to scan for weaknesses.

If you continue using Windows Server 2016 past the extended support dates, you may need to purchase 'Extended Security Updates.' While Microsoft offers this service, it is extremely costly, and the price rises each year, making it more a penalty for delay than a sustainable long-term solution.

Modernize Now

Concerned about the approaching Windows Server 2016 end-of-support deadline? We specialize in smooth migrations to the cloud and modern server environments. Let us take care of the technical heavy lifting, contact us today to begin your upgrade plan.

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.

POLICIES FOR EMPLOYEES WORKING FROM CAFES AND COWORKING 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.

HOW TO AUDIT YOUR MICROSOFT 365 COPILOT USAGE TO AVOID MASSIVE LICENSING WASTE

- **Conduct Regular Audits:** Perform audit to measure and quantify adoption rates.
- **Analyze User Activity:** Utilize the M365 admin center to track key usage metrics.
- **Identify Waste:** Distinguish between active users and employees who have limited or non-existent usage.
- **Optimize Licensing:** Reclaim licenses from inactive users and reallocate.
- **Formalize Requests:** Establish a formal request process for licenses, requiring employees to justify their need for the tool.
- **Continuous Review:** Treat IT budget optimization as an ongoing process with regular usage metrics review.
- **Address Training Gaps:** Survey staff to assess their comfort level and provide targeted training.
- **Boost Adoption:** Implement strategies like “lunch-and-learn” sessions or appointing “Copilot Champions.”
- **Set a Governance Policy:** Establish clear rules defining who qualifies for a license and setting expectations for usage and review cycles.
- **Plan for Renewal:** Schedule audits at least 90 days before renewal to allow time to adjust licenses counts and gain leverage in vendor negotiations.

Thank You!

Thanks for taking the time to read this month’s newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we’re only a phone call or email away.

MANAGEPOINT

manage-point.com

(414) 485-6169

dsteger@manage-point.com