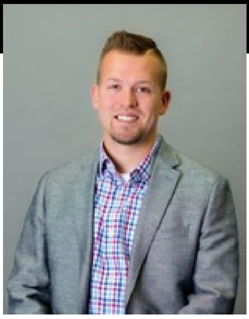
Virtual DataWorks

TECH BYTES

February 2026

FORTIFY YOUR FEBRUARY.
PROTECT YOUR BUSINESS.



Keep February Strong by Prioritizing Smart Cybersecurity for Your Business.

Matthew DeWees
-President

Cybercriminals have a new weapon: the Deepfake CEO Scam. For years, fraudsters used phishing emails to trick employees into sending money.

Now, AI lets them clone voices with alarming accuracy, using audio from webinars, social media, or voicemail greetings.

Here's how it works: An employee gets an urgent call or voicemail from someone who sounds exactly like the CEO or CFO, demanding a confidential wire transfer. The voice is convincing, and the urgency pushes employees to skip security checks.

How to protect your business:

- Adopt a "verify first" policy. Legitimate executives won't mind if you hang up and call back on a known number.
- Use verbal challenge passwords or safe words for sensitive transactions that AI can't fake.

Need help updating verification protocols or training staff? Contact us at everythingit@virtualdataworks.com to secure your communications.

Matthew DeWees

President

WHAT'S INSIDE?

DID YOU KNOW?

Romance scams cost victims over $1 billion a year. Love can be risky online! Always verify before you trust and never share sensitive info with a "secret admirer."

Virtual DataWorks
475 Wolf Ledges Parkway
Akron, Ohio 44311
virtualdataworks.com
(330) 800-2186

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.

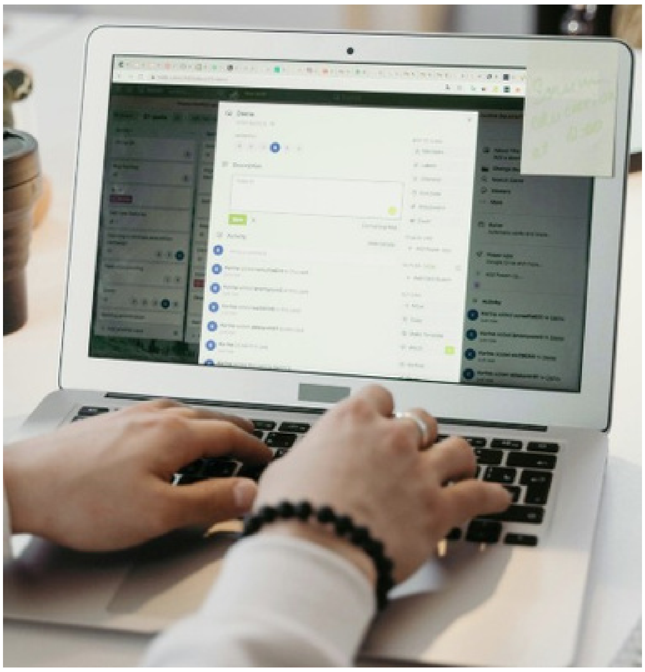
HOW AI VOICE CLONING SCAMS ARE CHANGING THE THREAT LANDSCAPE

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

Business email compromise (BEC) traditionally relied on phishing or domain spoofing to trick employees into sending money or sensitive data. These text-based scams were easier to block with email filters, and while still common, they’re harder to execute today. Voice cloning changes the game, adding urgency and trust that bypasses those defenses.



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.

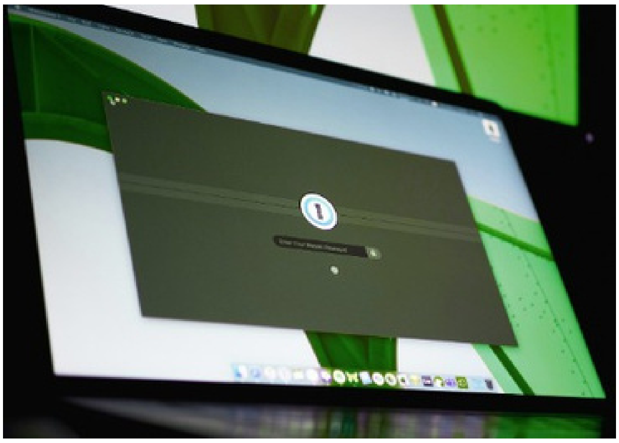
One of the more prominent standards used for such authentication is Fast Identity Online2 (FIDO2) open standard, that uses passkeys created using public key cryptography linking a specific device to a domain. Even if a user is tricked into clicking a phishing link, their authenticator application will 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

Passkeys are secure digital credentials stored on your device and protected by biometrics. They resist phishing, sync across platforms like iCloud Keychain or Google Password Manager, and combine hardware-level security with the convenience of your everyday device.

READ MORE

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:** Issueandrequire theuseof privacy screens to prevent passersby from glancing and stealing sensitive information.

- ✓ **Maintain Physical Security:** Employees mustkeeptheir laptops and devices with them at all times.

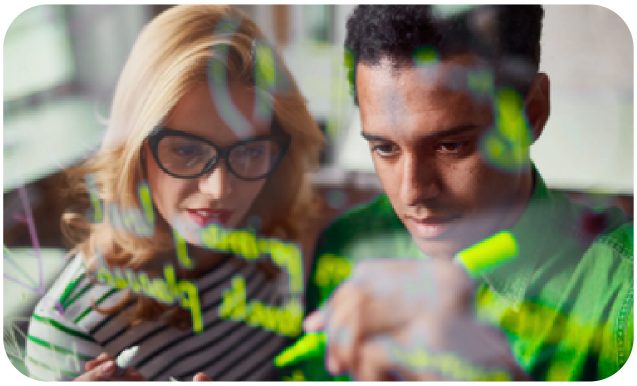
- ✓ **Avoid Confidential Conversations:** Employeesshould not discuss sensitive business matters in public.

- ✓ **Create a Clear, Written Policy:** Publish acomprehensive remote work policy and set a regular review cadence.

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

Streamline Your IT Budget and Licensing

Virtual DataWorks helps you audit Microsoft 365 Copilot usage to prevent costly licensing waste. Our team reviews licenses, analyzes real usage, and removes unused seats, ensuring your subscriptions match business needs and deliver maximum value.



OUR SERVICES INCLUDE:

- ✓ Cloud Solutions & Migration
- ✓ Cybersecurity Assessments
- ✓ Managed IT Services

LEARN MORE

Thank you for taking the time to read February's newsletter! We hope you discovered a few helpful tips and ideas to make your technology work smarter for you this month.

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

CONTACT US BELOW

☎ (330) 800-2186

✉ everythingit@virtualdataworks.com

🌐 virtualdataworks.com

📍 475 Wolf Ledges Parkway
Akron, Ohio 44311

Virtual DataWorks