

Serving our customers

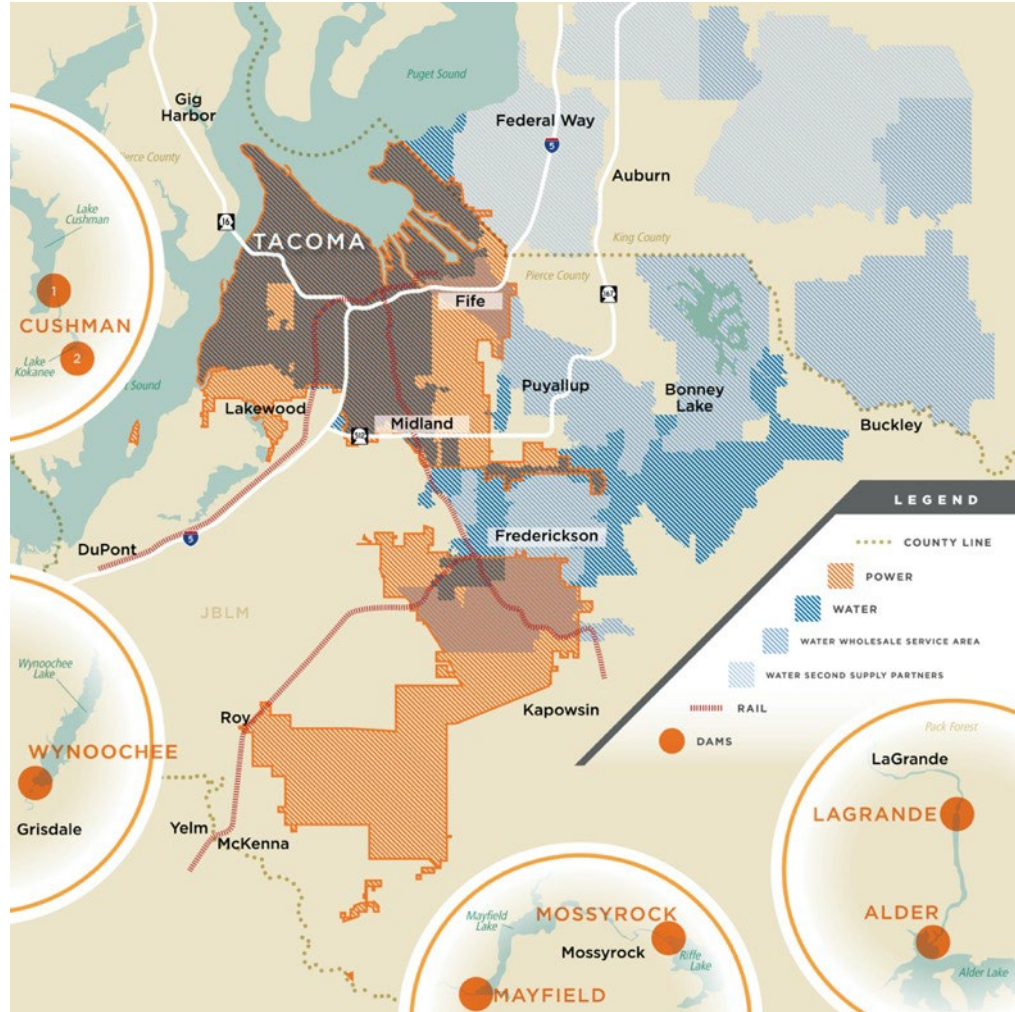
Cybersecurity Update & Training

Nate Walters, Cybersecurity Operations Manager

Ken Ake, CIP Training & Cybersecurity Awareness Program Manager

Public Utility Board Study Session · 2026-10-14

Agenda



- In the News: Midwest Water Utility Attacks
- In the News: AI and Cybersecurity
- How We're Responding
- Cybersecurity Awareness Training

Water Utility Attacks: What Happened



BOTTOM LINE In late July, attackers reached internet-exposed control equipment at water systems in at least seven states. Operators restored control within hours; Minnesota reported no impact to water quality.

CONFIRMED BY STATE

30+

Minnesota communities disrupted

July 26–27 · Braham, Plymouth, South St. Paul, Maple Plain named

CONFIRMED BY FBI / EPA

7+

states reported incidents to the FBI

as of July 30 · federal public alert

MEDIA REPORTED · AUG 4–6

12+

states affected in media reporting

incl. Michigan (9 systems), Georgia, New Jersey, South Dakota



Apr 7

CISA issues advisory AA26-097A on Iranian-affiliated PLC targeting



Jul 22

Advisory updated, four days before the attacks



Jul 26–27

Coordinated disruptions at Minnesota water systems



Jul 30

FBI and EPA public alert: at least seven states



Aug 1–6

Michigan, Georgia and other states confirmed in reporting

Source: Tenable, "Coordinated Cyberattack on Minnesota Water Utilities" (updated Aug 10, 2026), citing Minnesota IT Services, FBI/EPA PSA I-073026-PSA, CISA AA26-097A, ABC News and CBS News.

How the Attacks Worked

HOW THEY GOT IN



Exposed to the internet

Control equipment was reachable directly from the public internet.



Weak or default passwords

Little stood between an attacker and the controls.



Settings changed remotely

Attackers changed passwords and settings, locking operators out.

WHAT IT CAUSED



Manual operations

Utilities ran hands-on; most restored control within hours.



Pressure loss and flooding

Some plants briefly shut down or lost automated control.



No water-quality impact in MN

Boil-water notices were reported at some utilities elsewhere.

The takeaway: these attacks were not sophisticated. The exposure was the vulnerability.

Attribution: the pattern is consistent with CyberAv3ngers, a group the U.S. has tied to Iran's IRGC. Officials have not publicly attributed the July attacks.

What This Means for TPU

BOTTOM LINE The conditions behind these attacks are the conditions our architecture is designed to prevent.



Not on the internet

Our control systems sit on isolated, segmented networks with no direct path from the internet.



One controlled way in

Remote access requires multi-factor authentication, passes through a secured gateway, and every session is recorded. Vendors follow the same path.



Watched continuously

Our public-facing edge is scanned continuously with CISA. Purpose-built monitoring inside Water's control network arrives this year.

What we are not claiming: no utility is unbreachable. Our claim is narrower and stronger - the access pattern used in these attacks does not work against TPU.

AI and Cybersecurity: By the Numbers



BOTTOM LINE Attackers use the same AI tools we do, and it is making them faster, more scalable, and more convincing.

89%

increase in attacks by AI-enabled adversaries, year over year

29 min

average time for criminals to move from first access to spreading through a network

48 hrs

window in which 88% of vulnerabilities with public exploit code were attacked

2×

growth in voice-phishing intrusions in the first half of 2026

Last year: AI was elevating phishing. **This year:** it is elevating every stage of an attack.

Sources: CrowdStrike 2026 Global Threat Report (Feb 2026); CrowdStrike 2026 Threat Hunting Report (Aug 2026). Vendor-reported figures — verify before presenting.

What AI Changes for Attackers

SPEED

Weaknesses move from public disclosure to active attack in hours or days, not weeks. The window to patch is shrinking.

SCALE

AI agents automate reconnaissance and intrusion. In late 2025, a state-sponsored group used an AI agent to carry out most of an espionage campaign against about 30 organizations.

DECEPTION

Flawless phishing emails, cloned voices, and deepfake video. The FBI has warned of AI-generated voice messages impersonating senior U.S. officials.

Connecting the two stories: the July water attacks needed no AI. But AI lowers the skill and time required to find and exploit exposed systems like those — at scale.

Sources: Anthropic, "Disrupting the first reported AI-orchestrated cyber espionage campaign" (Nov 2025); FBI IC3 PSA on impersonation of senior U.S. officials (May 2025). Verify before presenting.

How We're Responding



Detection and Response

- Analysts monitoring and responding to alerts
- Endpoint detection and response
- OT network monitoring: Water in 2026, CIP-015 scope by 2028



Managing Vulnerabilities

- Risk-based vulnerability management
- Continuous external attack-surface scanning
- Faster remediation as exploit windows shrink



Secure by Design

- Network segmentation
- Security design reviews for major projects
- Third-party testing before go-live for high-value systems



Practice and Partnerships

- Annual tabletops expanding to Water (2026) and Rail (2027)
- Intelligence sharing: CISA, FBI, WA National Guard, LPPC

Cybersecurity Is a Team Sport

Cybersecurity Awareness Training

Ken Ake, CIP Training & Cybersecurity Awareness Program Manager

It has never been easier to be you

2026 Cybersecurity Awareness Training

UTS Cyber & Resilience



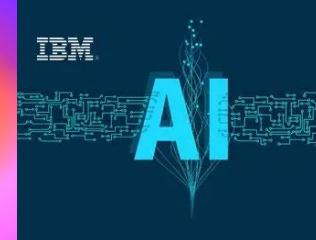
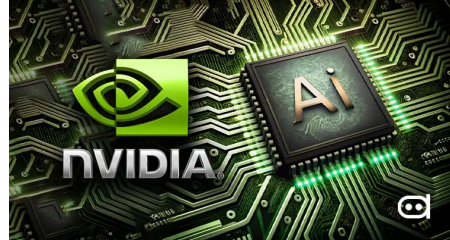
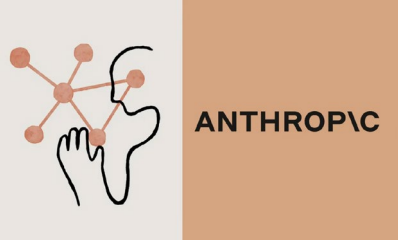
Agenda



- Information Mosaics
- New & Old Methods of Attacks
- An Attack Sequence
- Takeaway

Information Mosaics





What does your AI assistant know about you?

What the AI in Microsoft 365 can reach

- Your email and calendar.
- Teams' chats, meetings and their transcripts.
- Every file you can open, including ones you never knew you could.
- On some new Windows PCs, an optional feature that snapshots your screen every few seconds and makes it searchable.

Why That Matters

- One prompt replaces a week of reading. Whoever holds your login holds the summary.
- Oversharing that used to be invisible is now one question away.
- Personal AI apps are not private by default: in 2025, "shared" ChatGPT chats turned up in Google, and Meta AI published conversations users thought were private.



The Picture AI Builds of you

Public, or already leaked

- Your TPU bio and photo; your LinkedIn history.
- Hours of meeting video: your face, your voice, how you talk.
- Property, campaign-finance and court records; social media.
- Breach data, such as 340,000 Pierce County library patrons' names and birthdates (2025).



AI, MINUTES

The attacker's brief (composite, no real person person)

Board member. Retired engineer; former county employee. employee. Answers email from a phone, evenings. Defers to Defers to the Chair; trusts the Director's office. Two grandchildren, school named on Facebook. Voice sample: 6 sample: 6 hours.

Pretext: "Hi, it's [assistant] in the Director's office. The Chair Chair asked me to get you the revised packet before tonight's tonight's session. Which number should I text the secure link secure link to?"



A study published in June 2026: AI built accurate target profiles from public data 88% of the time, and its automated automated spear-phishing matched human experts. 54% clicked, versus 12% for generic phishing.

The New Old Phish

ClickFix, in three keystrokes

Verify you are human

To continue, complete these steps:

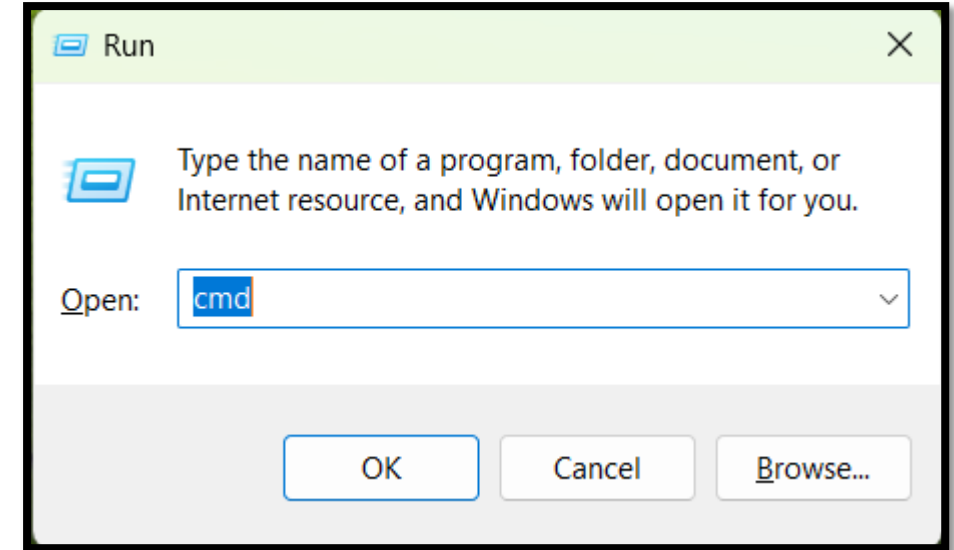
1. Press Windows + R · 2. Press Ctrl + V · 3. Press Enter

- The page silently copied a command to your clipboard. Step 3 runs it, with your permissions.
- Security tools see you typing, not malware arriving. That is why it works.
- Mac Also has similar attacks as well.

Why it is everywhere

+517%

growth into the first half of 2025, then another +108% into the first half of 2026.



No real verification, update or error message asks you to open Run, Terminal or PowerShell and paste a command. If "IT" calls you on Teams for remote access, hang up and call the Service Desk number you already have.

Extract Audio from Your YouTube Videos for High-Fidelity Sound

Convert your YouTube videos into high-quality audio files. Upload your video to extract the audio, enhance the sound quality, and download it as an MP3 file directly from your browser.

 Paste a video link

Download video

Over 1 million creators use Flixier every day including brands like:



Bringing technology to life

Powering the best enterprises, creators, and developers. From ElevenAgents for customer experience, ElevenCreative for content creation, to the leading AI voice generator.

Sign up

Contact sales

ElevenCreative

ElevenAgents

ElevenAPI

Preview Original

Preview Clone

AI Voice Generator

Text to Speech

Music

Speech to Text

Voice Cloning

Dubbing

Sign up

Free AI Face Swap

Swap faces in photos, videos, or GIFs—free, no sign up.

Photo Face Swap

Video Face Swap

GIF Face Swap

1

FaceHeadBody

Upload original photo

Choose the photo whose face you want to replace.

2

SingleMulti

Upload replacement face

Choose a clear photo of the face you want to add.

5 Images left today

Swap Faces



EXPLOITING MICROSOFT TEAMS: IMPERSONATION AND SPOOFING VULNERABILITIES EXPOSED

Google Chrome

Something went wrong while displaying this webpage.

There was an error during the latest update of browser version, causing some web pages to malfunction.

Follow these instructions to resolve the issue:

1. Click the 'Copy fix' button below.

2. Right-click on the Windows icon

3. Select 'Windows PowerShell (Admin)'

4. Right-click within the open terminal window.

5. Wait for the update to complete, then refresh the page.

Copy fix

Close

facebook

facebook

Welcome to Facebook! Here you can make new friends, connect, and build meaningful relationships. Join our community to stay updated on all events and meetups.

Press the key combination **Ctrl + R**, then **CTRL + V**, and press **Enter**.

Fix it

Retry

Powered by Facebook

PDF Simpli

Our website makes file conversions for PDF's quick and simple. Just upload a PDF or another document type to get started.

Your browser does not support correct upload files. Please follow the instructions below using the "Fix it" button.

Fix it

Retry

Powered by PDF-Simpli

Verify You Are Human

Please verify that you are a human to continue.

I'm not a robot

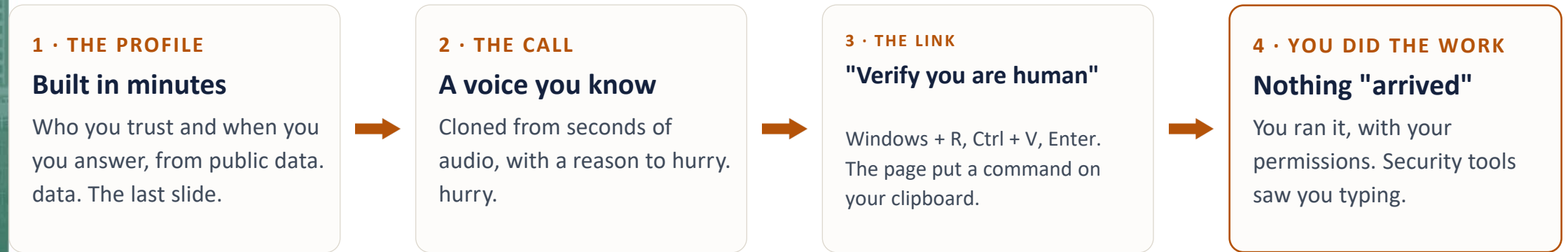
Verification Steps

1. Press Windows Button **Win** + **R**

2. Press **CTRL** + **V**

3. Press **Enter**

How it comes together



▶ *"Hi, it's [assistant] in the Director's office. The Chair asked me to get you the revised packet before tonight's session. Which number should I text the secure link to?"*

47% of Microsoft's initial-access cases in 2025 started with step 3 · +517% in a year, then +108% more · the kit rents for about **\$380 a month**.

⚠ **A voice is not proof: hang up and call back on a number you already have. No real verification, update or error message asks you to paste a command. Use more disruptive prompts if needed.**

Why does this matter?

In 2020, to become you an attacker needed

- Weeks of research, by hand.
- A fluent writer who knew how you talk.
- A convincing caller, or no phone call at all.
- Someone who could break in.

In 2026

- Minutes: AI builds the profile from public data, accurate 88% of the time.
- AI writes in your voice; 54% click, the same rate as human experts.
- A voice clone from a few seconds of meeting video.
- No break-in needed: you paste the command or approve the remote session.



The cost of becoming you collapsed. The cost of stopping it did not: four habits.



Lock it

MFA on every account you use for board business, and on your personal email, which is the recovery path for everything else.

Shrink it

Tighten social-media privacy; keep family, schools and travel off public posts; opt out of people-search sites. Board business stays on your TPU account and approved tools, never a personal AI app.

Verify it

Urgent request by text, email, email, voice or Teams? Hang up and call back on a number you already have. Never paste a command you were sent; never approve a remote session you did not ask for. Utilize disruptive prompts.

Report it

A click, a strange call, a pasted command, a lost device: tell us the same day. No embarrassment required.



Questions & Feedback