Think before you click!

Ohio Court Reporters Association · Matt Lydy · 2026

Today's Agenda

01 Email & Phishing

02 Passwords & 2FA

03 Passkeys — The Future

04 Ransomware & Backups

05 New Threat Vectors

06 Your Car Is Spying On You

07 Privacy.com

08 AI: Threats & Staying Safe

09 Wrap Up & Resources

01

Email & Phishing

Your inbox is the front door. Hackers knock here first.

EMAIL SECURITY

Email Is Your Digital Identity Hub

Master Key to Everything

If a hacker owns your email, they own your bank, medical records, and social media. They just hit 'Forgot Password' on every site you've ever used.

Phishing is the #1 Attack Vector

Attackers impersonate banks, courts, or colleagues. One convincing email, one click, and your entire practice is exposed.

Use Separate Email Accounts

Professional work · Financial accounts · Subscriptions & junk. Compromise one, not all. It's the digital equivalent of not keeping all your eggs in one basket.

Always Enable MFA on Email First

Before anything else on today's list — go home and turn on multi-factor authentication on your email. This is the single highest-impact thing you can do today.

EMAIL SECURITY

How to Spot a Phishing Email

Urgency & Fear

"Your account will be suspended in 24 hours!" Attackers want panic. Panic = no thinking = click.

Mismatched Sender Address

Display name says 'Chase Bank' — actual email is chase-alert@gmail.ru. Always check the real address.

Hover Before You Click

Hover over any link first. Does the URL match where it claims to go? No? Don't touch it.

Generic Greetings

"Dear Customer" instead of your name. Banks and courts know who you are. Attackers don't.

Unexpected Attachments

Never open .zip, .exe, or .docm files you weren't expecting. Even PDFs can be weaponized now.

Requests for Credentials

No legitimate org — ever — will ask for your password via email. If they do, it's a scam.

🎣 **Pro tip: When in doubt, go directly to the website by typing the URL yourself. Never click. Never assume.**

EMAIL SECURITY

Spot the Phish — Side by Side

Suspicious email

From: “Assoc. Services” <info@memberportal-alerts.net>

Subject: ACTION REQUIRED: Verify your account now

Dear Member, your account requires immediate verification. Failure to verify within 24 hours will result in suspension and loss of conference access.

Verify My Account Now

`memberportal-alerts.net/verify-login`

Red flags: Wrong domain | Generic greeting | Fake urgency | Hidden URL

Legitimate email

From: Member Services <info@nationalassoc.org>

Subject: Your 2025 conference registration is confirmed

Hi Sandra, thank you for registering for the 2025 Annual Conference. Your spot is confirmed. Questions? Reply to this email or log in to your member portal.

View my registration

`nationalassoc.org/my-account`

Green flags: Real domain | Uses your name | No urgency or threats | Clean URL

Illustrative example only. All names, organizations, and domains are fictional and used for educational purposes.

🔍 **The #1 rule: hover over ANY link before you click. The real destination URL never lies.**

NEW THREATS

AI-Powered Phishing — Not Your Grandpa's Nigerian Prince

BEFORE AI — Easy to Spot

DEAR FRIEND,

I am the son of a Nigerian prince. I am needing help to transfer $47,000,000 USD from my country. You will recieve 30% commision. Please sending me your bank account number urgently. This is very legitimate.

God bless,
Prince Adewale Okonkwo III

❌ Poor spelling ❌ Generic greeting
❌ Ridiculous premise ❌ Easy to dismiss

AFTER AI — Terrifyingly Convincing

- Personalized with your real name and employer
- References real events (your conference, your software vendor)
- Perfect grammar and professional tone
- Mimics the exact writing style of people you know
- Uses your public social media against you
- Tailored to your specific role and concerns
- Generated in seconds, for thousands of targets simultaneously

We just built one. You saw it. It took 15 seconds.

02

Passwords & 2FA

The locks on your digital life — are they any good?

PASSWORDS

Password Mistakes — Stop Doing These

✗	**123456 / password / OCRARULES2026**	⚠ Cracked in under 1 second by automated tools
✗	**Reusing the same password everywhere**	⚠ One breach exposes ALL your accounts
✗	**Sharing passwords with colleagues**	⚠ Creates liability — you can't audit who did what
✗	**Writing passwords on sticky notes**	⚠ Physical theft = instant access. Yes, someone will look.
✗	**Never changing after a breach**	⚠ Breaches are often discovered months — or years — later

The Solution: Password Managers

How They Work

- You remember ONE master password — it handles all the rest
- Auto-fills logins on websites and apps automatically
- Generates strong, unique, random passwords for every site
- Alerts you when passwords appear in known data breaches
- Shows every site where you've reused a password (brace yourself)
- Syncs across all your devices — phone, tablet, computer

Matt's Pick

1Password

1password.com

✓ Works on Mac, PC, iPhone & Android

✓ Family & Business plans available

✓ Secure document storage included

✓ I personally use this every day

💡 **Great password tip: “March 2026 OCRA ruled!" — Easy to remember, incredibly hard to crack. Spaces and punctuation are your friends.**

PASSWORDS

Two-Factor Authentication — and Its Achilles Heel

99.9%

of automated attacks blocked by MFA

— Microsoft Research

SMS Text Code

A one-time code texted to your phone. Better than nothing — but see below.

Authenticator App

Google or Microsoft Authenticator. Rotating 6-digit code. Much stronger than SMS.

Hardware Key / Biometric

Physical USB key (YubiKey) or fingerprint. Gold standard. Nearly impossible to remotely defeat.

⚠ The SMS Problem — SIM Swapping

A hacker calls your carrier, pretends to be you, and convinces them to transfer your phone number to their SIM card. Every text-based 2FA code now goes to them. The FBI reported nearly $26 million in US SIM swap losses in 2024 alone — and UK cases surged 1,055% in 2024. In March 2025, T-Mobile was ordered to pay $33 million in a single SIM swap case.

03

Passkeys — The Future Is Here

Your iPhone or Android already uses them. Passwords are on their way out.

Passkeys — Passwords Are Dying (Finally)

What is a Passkey?

A passkey replaces your password entirely. Instead of typing something you know, you prove who you are using something you are — your face, fingerprint, or device PIN.

Your device generates a unique cryptographic key pair. The private key never leaves your device. The website only stores the public key. There is no password to steal.

Apple, Google, and Microsoft are all pushing this standard hard right now. Many sites already support it.

Why it's better:

- ✓ **Can't be phished — there's nothing to type and steal**
- ✓ **Can't be breached — no password stored on a server**
- ✓ **Can't be guessed — it's cryptographic, not memorable**

Who supports Passkeys today?

- ✓ Apple (iPhone, Mac, iPad)
- ✓ Google (Gmail, Android)
- ✓ Microsoft (Windows Hello)
- ✓ Amazon, PayPal, GitHub
- ✓ 1Password stores passkeys too!

PASSKEYS

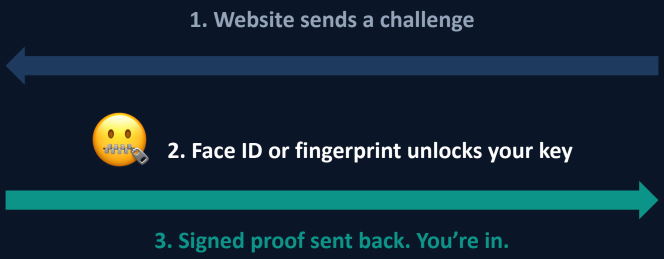
How a Passkey Works

Two keys are created as a matched pair. One stays with you. One goes to the website. Neither works without the other.

📱 YOUR PHONE

PRIVATE KEY

- ✓ Locked inside your phone
- ✓ Never sent anywhere — ever
- ✓ Unlocked by your face or fingerprint



1. Website sends a challenge

2. Face ID or fingerprint unlocks your key

3. Signed proof sent back. You’re in.

✓ No password ever typed or sent

🌐 THE WEBSITE

PUBLIC KEY

- ✓ Stored on the website’s server
- ✓ Verifies the signed proof from your phone
- ✓ Useless to hackers without your phone

🔒 **The hacker’s nightmare: even if they steal the website’s entire database, all they get is the public key. It’s like stealing a padlock with no key — completely useless.**

04

Ransomware & Backups

The threat is real. Your only defense is a copy you made yesterday.

RANSOMWARE

How Ransomware Works — The 4-Step Nightmare

1

You Click a Link

A phishing email or bad website silently installs malware on your machine.

2

Silent Encryption

Ransomware quietly encrypts ALL your files — transcripts, billing, photos, local backups — while you work normally.

3

Spreads the Network

If you're on a shared network, it jumps to other computers and servers.

4

Ransom Note Appears

A screen demands Bitcoin payment — often $500–$50,000+. Even if you pay, recovery is NOT guaranteed.

Ransomware attacks surged 485% in 2020 · Average victim cost: $847 + 23 days downtime · $1.1 billion paid in ransoms in 2023

RANSOMWARE

BACKUP YOUR COMPUTER — This Is Non-Negotiable

The 3-2-1 Backup Rule

3 copies of your data

2 different storage types (local + cloud)

1 copy offsite — cloud counts

Matt's Pick

Backblaze

backblaze.com · ~$99/year

📱 **Scan this QR code for a Backblaze free trial!**

SCAN ME

⚠ **Wait. I'm about to tell you on the very next slide...**

...don't scan random QR codes.

This one is safe, I promise. But that's exactly what a hacker would say. 😄

NEW THREATS

QR Code Scams — What Actually Happens When You Scan

I told you not to scan random QR codes. Here's exactly why:

Fake Websites

Scan takes you to a cloned version of a real site — parking app, restaurant menu, bank login. You enter your credentials. They go to the attacker.

Malware Download

Scanning triggers an automatic download of malicious software onto your phone. No click required beyond the scan itself.

Quishing (QR Phishing)

QR codes in emails bypass most corporate email security filters — they can't 'see' a QR code the way they can scan a URL. Used specifically to evade security tools.

Parking Meter Scams

Fake QR code stickers placed over real ones on parking meters. Nationwide problem. You pay — but to the scammer, not the city.

Package Delivery Scams

"Scan to reschedule your delivery" — there is no package. Just a credential-harvesting page designed to look like FedEx or UPS.

Conference & Event Scams

Fake QR codes placed on signage at events. Someone could literally put a sticker over a legitimate QR code at THIS conference today.

05

New Threat Vectors

The threat landscape has changed. Here's what's new and nasty.

NEW THREATS

Data Brokers — Your Personal Info Is For Sale Right Now

Search your own name on any of these sites. You might not like what you find.

What Data Brokers Know About You

- Full name + every address you've ever lived at
- Phone numbers (current and historical)
- Family members' names and relationships
- Political affiliation and voting history
- Estimated income and net worth
- Property records and vehicle ownership
- Criminal and court records
- Social media profiles and activity

What You Can Do

Search yourself on Spokeo, WhitePages, BeenVerified — know what's out there

Submit opt-out requests to each broker (tedious but effective)

DeleteMe.com (~$129/yr) automates opt-outs for you

Know that SIM swap and spear-phishing attacks use this data as fuel

Why this matters to court reporters specifically: Your home address, schedule patterns, and client relationships are often in these databases.

NEW THREATS

Fake Invoice & Payment Fraud — Targeting Practices Like Yours

Solo and small firm practitioners are the #1 target for payment fraud. Here's why:

Common Attack Scenarios

The 'Updated Banking Details' Email

A trusted vendor or attorney emails you — from a spoofed address — saying their payment details have changed. You pay the new account. They never get the money.

Fake Software Renewal Invoice

An invoice that looks exactly like your transcript software or court filing service arrives. You pay it. It's not real. The real bill is still coming.

Business Email Compromise (BEC)

Hackers sit silently in your email for weeks reading your conversations. Then they impersonate you — or someone you trust — at exactly the right moment.

Protect Yourself

✓ Verify ALL payment changes with a phone call — not email reply

✓ Call the number you already have, not one in the suspicious email

✓ Enable fraud alerts on all business banking

✓ Use Privacy.com virtual cards for vendor payments

✓ Never pay an invoice you weren't expecting without verification

06

Your Car Is Spying On You

The privacy nightmare nobody is talking about — until now.

CAR PRIVACY

What Your Connected Car Is Collecting (And Selling)

"Sitting in a connected car is a lot like handing your phone over to the auto manufacturer." — Mozilla Foundation

What They Collect — From ALL 25 Major Brands

- 📍 Precise location history — everywhere you go
- 🎙️ Voice recordings from in-car microphones
- 📱 Phone contacts, texts synced via Bluetooth
- 🌐 In-car browser and app history
- 🧬 Genetic information (6 brands admitted this)
- 💊 Health and medical data
- 🗳️ Political and religious beliefs
- 😳 Sexual activity (yes, Nissan's policy says this)

The Numbers

25/25	brands FAILED Mozilla privacy tests
84%	sell or share your data with third parties
56%	share with law enforcement on informal requests — no warrant needed
0%	encrypted the personal data they collect

💥 Real Story: A Toyota owner's driving data was shared with Progressive Insurance without clear consent. His insurance rate increased 21%. He only found out by accident. This is happening now.

CAR PRIVACY

And By The Way — You've Been Working For Them For Years

🤖 The reCAPTCHA Twist

Every time you solved a reCAPTCHA puzzle — 'select all the traffic lights,' 'identify the crosswalks,' 'click every fire hydrant' — you were annotating images for AI training datasets.

Those images? Primarily from street-level photography used to train autonomous vehicle and mapping AI.

Google acquired reCAPTCHA in 2009. Hundreds of millions of users. Billions of labeled images. You did this for free. Google built products worth billions from it.

You were unpaid AI training labor.

You're welcome, Silicon Valley. 🤷‍♂️

Protect Your Car Privacy

✓ Read what you're signing up for with 'Connected Services' — there is usually an opt-out

✓ Don't connect your phone contacts to rental or borrowed cars

✓ Factory-reset any vehicle you sell — your data stays in the system otherwise

✓ Be aware your driving behavior may be shared with insurers

✓ Call your insurer and ask if they receive telematics data from your car manufacturer

✓ Visit your car manufacturer's privacy portal and request a data access report

💡 **Source: Mozilla Foundation 'Privacy Not Included' study — all 25 major car brands tested received failing marks. First time in the study's 7-year history.**

07

Privacy.com — Your Payment Shield

I use this every single day. Here's why you should too.

PRIVACY.COM

Privacy.com — Matt Uses This Every Day. Here's Why.

> *"I use Privacy.com for every online subscription and vendor payment. It generates a virtual card number that links to my real account — but the merchant never sees my actual card. If they get breached, or if I want to cancel, I just close that virtual card. Done. My real account is untouched."*

Locks to One Merchant

Each virtual card only works at the site it was created for. Stolen card number goes elsewhere? Declined instantly. Useless to attackers.

$ Set Spend Limits

Cap what any merchant can charge you. Perfect for subscriptions that mysteriously increase their price hoping you won't notice. You'll notice.

✖ Pause or Close Anytime

Cancel a virtual card in seconds from your phone. No hold music. No 'retention specialist.' No 45-minute wait. Just close it.

PCI-DSS + SOC 2 Certified

Bank-level security. 256-bit encryption. Has processed over $3 billion in transactions. Free to start — 12 virtual cards/ month at no cost.

💼 **Court reporter use cases: Transcript software subscriptions, court filing fees, research databases, conference registrations, one-time vendor payments**

08

AI: Threats & Staying Safe

Light touch — you're smart enough to know the basics by now.

AI THREATS

How AI Is Being Used Against You Right Now

AI can clone a voice from as little as 3 seconds of audio — a social media video, a voicemail. 'Mom, I'm in trouble, I need money' — may not be your kid. Verify with a family code word.

Deepfake Video Evidence

AI-generated video and audio are increasingly being submitted as evidence. Courts are only beginning to grapple with authentication. As court reporters, this is your world.

AI-Personalized Phishing

We built one earlier. Perfectly written, perfectly targeted, using real information about you from public sources. Old detection methods don't work. Behavior matters now.

Impersonation at Scale

AI allows criminals to convincingly impersonate colleagues, vendors, and authorities in real time — text, email, and increasingly voice calls. When in doubt, verify out-of-band.

🔑 **The family safe word: Pick a word or phrase your family uses to verify identity in an unexpected call. 'Are you really you? What's our word?' Sounds silly. Saves thousands of dollars.**

AI SAFETY

Using AI Tools Safely — The Short Version

✓ Safe to Use AI For

✓ Drafting and editing non-confidential correspondence

✓ Research and summarizing public information (verify sources)

✓ Learning — tutorials, explanations, definitions

✓ Proofreading and grammar checking your own writing

✓ Automating repetitive admin tasks like scheduling and templates

✓ Analyzing the phishing emails you receive 😄

✗ Never Do These

✗ Enter client names, case numbers, or testimony into public AI tools

✗ Accept AI-generated legal citations without verification — they hallucinate cases

✗ Treat AI transcription as certified without your review and signature

✗ Assume any AI-generated image, audio, or video is authentic

✗ Ignore the output just because it sounds authoritative and confident

DIGITAL RIGHTS

When Legislators Write Laws About Tech They Don't Understand

California AB-2047 and Washington HB-2321 — A Case Study in Clumsy Digital Legislation

What These Bills Do

Both bills attempt to criminalize the possession of digital files that could potentially be used to 3D-print certain parts — even if those files have entirely legitimate uses.

The core problem: a simple spring-shaped file, a cabinet hinge design, an architectural component — the technology literally cannot determine intent from geometry. The law criminalizes ambiguity.

California AB-2047 goes further — it would require DOJ-approved 3D printers to maintain internal surveillance logs of printing activity and potentially report 'suspicious' prints to state authorities.

Washington HB-2321 mandates blocking features that users cannot override, even with 'significant technical skill.'

Why You Should Care

If a device you OWN can be required to surveil and report your activity to the government — what stops that precedent from spreading?

The same logic applied to your laptop: 'this file COULD be misused' covers enormous territory

Legislators writing laws about files and formats they don't understand have already passed laws affecting your work

Courts are already wrestling with AI-generated evidence — vague tech laws make this worse, not better

The question isn't about any specific use case — it's about the precedent of mandating surveillance software inside devices you own and criminalizing files based on theoretical misuse.

Your Personal Security Checklist — Take One Action Today

□ Passwords

Set up 1Password — migrate your passwords this week

□ SIM Safety

Call your carrier and set a SIM lock PIN on your account

□ Privacy

Create a Privacy.com account for your next online payment

□ Data Brokers

Search yourself on Spokeo — see what's out there

□ Security

Enable 2FA on email using an authenticator app (not SMS)

□ Backups

Install Backblaze — set it, forget it, sleep better

□ Social

Set all social media profiles to Private

□ Car Privacy

Factory reset any car you sell — your data is on there

Recommended Resources & Links

Passwords

1Password

1password.com

Matt's pick — password manager

Backup

Backblaze

backblaze.com

Unlimited cloud backup ~$99/yr

Privacy

Privacy.com

privacy.com

Virtual cards — free plan available

Antivirus

Bitdefender

bitdefender.com

Top-rated malware & ransomware protection

VPN

Private Internet Access

privateinternetaccess.com

VPN for public WiFi safety

Data Brokers

DeleteMe

joindeleteme.com

Automated data broker opt-outs

Breach Check

Have I Been Pwned?

haveibeenpwned.com

Check if your email is in a breach — free

AI Tool

Claude

claude.ai

What you saw today — responsible AI assistant

Stay Safe. Stay Certified. Stay Irreplaceable.

The best security tool in the room isn't any app or service.
It's the skeptical, well-informed human being using them.

Take one action today:

Install Backblaze + Set up 1Password + Create a Privacy.com account

Matt Lydy · Ohio Court Reporters Association · 2025 · Questions?