

# Join the Phishing Resistance!

Recap from the March 31, 2026 DelCor Client Education Network webinar.

*Drafted using Copilot; thoughtfully refined by an actual human.*

## Session Description

Phishing is no longer about spotting suspicious emails—it is about stealing identities. As associations rely on cloud platforms such as Microsoft 365, attackers increasingly target users to gain access to email, files, vendors, and financial systems.

---

## Key Takeaways

### 1. Phishing Targets People, Not Systems

Modern phishing attacks focus on user credentials—the fastest path to an organization's data. Even well-secured cloud environments are vulnerable if a single account is compromised.

### 2. MFA Alone Is No Longer Enough

Live demonstrations showed how attackers can bypass traditional multi-factor authentication (MFA) using real-time “man-in-the-middle” phishing techniques that capture login tokens.

### 3. The Most Dangerous Phishing Looks Legitimate

The most successful attacks often originate from trusted sources—vendors, colleagues, or shared files—because they bypass spam filters and rely on trust rather than obvious deception.

### 4. Passkeys Are the New Standard

Passkeys replace passwords and MFA codes with device-based authentication (PINs, biometrics, or security keys). They are:

- Phishing-resistant by design
- Not transmitted over the internet
- Easier and faster for users

### 5. Enforcement Is Essential

Passkeys must be required, not optional. Leaving legacy authentication methods enabled allows attackers to force users into weaker login paths.



## 6. Cyber Insurance Is Driving Change

Cyber insurers increasingly mandate security controls. Just as MFA became standard, passkeys are likely to become a future requirement as insurers respond to MFA-bypass attacks.

---

### Recommended Action Steps

#### ✓ Assess Your Risk

Review recent phishing attempts and sign-in activity to understand exposure to MFA-bypass attacks.

*Owner: IT / Security Team*

#### ✓ Plan for Passkeys

Confirm support for local passkeys (e.g., Windows Hello for Business) and portable passkeys (mobile devices or security keys).

*Owner: IT Leadership / Identity & Access Management*

#### ✓ Enforce Strong Authentication

Disable legacy authentication methods once passkeys are deployed to prevent downgrade attacks.

*Owner: IT Security Administrator*

#### ✓ Train for Verification

Require staff to verify unexpected file shares, invoices, or payment requests using a second channel (call or Teams message).

*Owner: All Staff (policy supported by leadership)*

#### ✓ Align With Cyber Insurance

Review cyber insurance requirements and proactively align authentication controls before they become mandatory.

*Owner: Executive Leadership, Finance, IT*

---

### About DelCor





DelCor Technology Solutions partners with associations to deliver secure, practical, and people-centered technology strategies. DelCor has fully implemented passkeys internally and recommends phishing-resistant authentication as a best practice for clients.

