corsica technologies

MANAGED SECURITY SERVICES

Attackers Are Bypassing MFA In Real Time.

The solution is **Phishing-Resistant MFA.**

How a modern attack slips past MFA:

STEP 1

The Lure

A trusted-looking email or Teams message delivers the hook.

STEP 2

The Fake Login

The user lands on a pixel-perfect copy of a real Microsoft login page.

STEP 3

The Real-Time Relay

The fake page captures all keystrokes and code while also relaying it to the real Microsoft login.

STEP 4

The Token Stolen

Microsoft issues a session token. The attacker steals it and logs in.

How phishing-resistant MFA stops these attacks:

Each credential is cryptographically bound to the real site's origin. A proxied login fails the binding, so the attacker **never receives a session token.**

$130K+

average loss from a single business email compromise

- Wire fraud
- Vendor impersonation
- Email & identity theft
- Ransomware entry

Easy authentication methods:

Passkeys MOST COMMON

On your device or authenticator. Any platform — a tap or biometric.

Windows Hello EASY WIN

Built into Windows — face, fingerprint or PIN. No phone needed.

Certificate-Based ENTERPRISE

Organization-controlled PKI for regulated environments. Maximum control.

A baseline security requirement.

CYBERSECURITY GUARANTEE

Now part of how we responsibly manage your environment. Clients below baseline may have the Cybersecurity Service Guarantee suspended for preventable incidents.

Book your MFA assessment Talk to your vCIO about scope, timeline, and Entra ID P1 licensing.

corsicatech.com sales@corsicatech.com (855) 411-3387