

Advisory: Credential Theft Bypassing MFA—What You Need to Know

TLP:CLEAR

REN-ISAC is tracking an increase in reports of reverse proxy-based phishing attacks that successfully bypass Multi-Factor Authentication (MFA). This threat has recently impacted multiple institutions across REN-ISAC membership and the broader research and education sector, targeting faculty, staff, and researchers. While MFA remains one of the most effective tools in protecting credentials, it is not foolproof, especially in the face of adversaries who adapt their tactics.

How the Attack Works

These attacks rely on malicious reverse proxy servers that sit between the user and the legitimate login page. The diagram below shows the attack chain where MFA is bypassed:

- User visits a phishing site mimicking their institution's login page.
- The phishing site proxies the user's credentials and MFA input to the legitimate site.
- The attacker receives a valid session cookie, bypassing MFA.
- The user is redirected to a benign or expected page, unaware of the compromise.

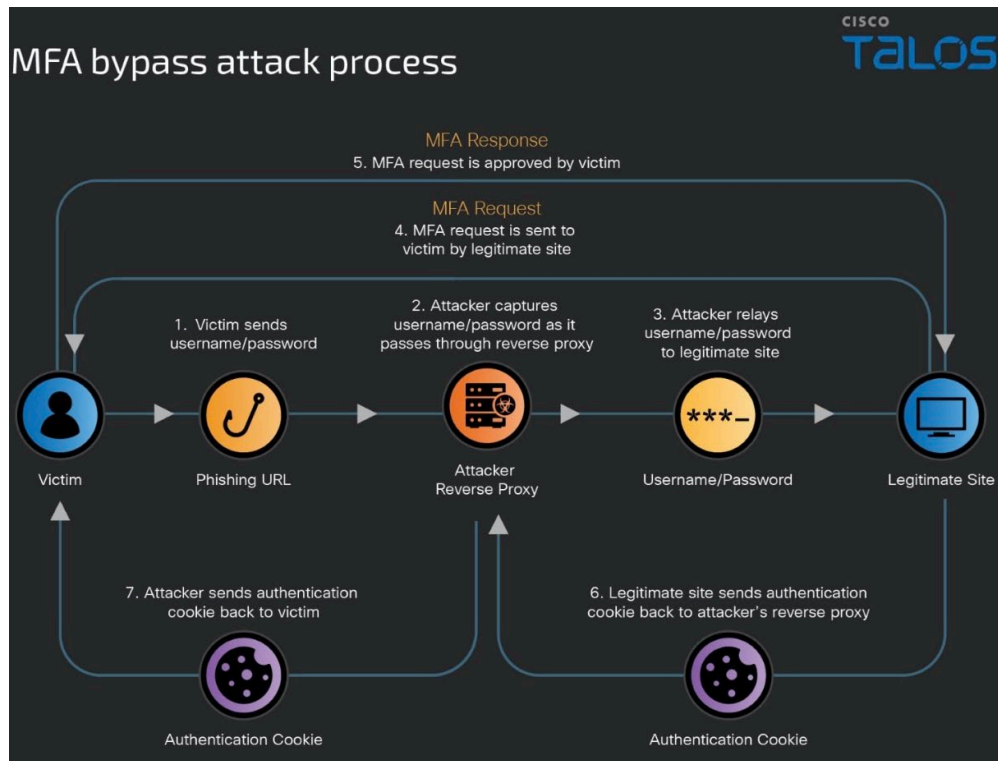


Figure 1: MFA bypass attack process flow chart. Credit: Cisco Talos

Why MFA Is Still Critical

MFA significantly reduces the risk of account compromise. Studies show that MFA blocks over 99% of automated attacks and most phishing-related breaches. However, adversaries are now using sophisticated proxy-based phishing sites to capture credentials and MFA tokens in real time, enabling full account access.

Why This Matters in Higher Ed & Research

Higher education and research institutions are prime targets for cyberattacks. They hold valuable intellectual property, sensitive personal data, and credentials with access to federal research. Complex IT environments, federated systems, and decentralized security controls increase the risk of lateral movement and data theft—even when MFA is in use.

Recommended Defensive Measures

- Use phishing-resistant MFA methods such as hardware security keys (e.g., YubiKey) or biometric verification.
- Enforce device-bound authentication using token binding or certificate-based trust models.
- Shorten session lifetime and implement anomaly-based session monitoring.
- Train users to recognize suspicious login pages and verify URLs before authenticating.
- Deploy threat detection systems that flag known proxy toolkits like Evilginx2, Modlishka, or Muraena.

Personal and Professional Protection

Encourage users to adopt MFA for both institutional and personal accounts. Many successful intrusions start with personal account compromise and spread into enterprise systems. Protecting email, banking, cloud, and social accounts helps reduce the broader attack surface.

REN-ISAC, OmniSOC, and MFA's Role in Threat Response

REN-ISAC strongly advocates MFA adoption across all accounts—academic, research, and personal. We provide guidance and threat intelligence that consistently shows MFA as a top preventive measure against account compromise

OmniSOC monitors member networks for signs of credential-based intrusions in real time. When MFA is in place, it often stops these attacks early, allowing analysts to focus on more advanced threats.

The combination of REN-ISAC's community intelligence and OmniSOC's operational vigilance builds stronger defenses across the higher education and research sectors.

Call to Action

MFA is not a silver bullet, but it is one of the most effective steps we can take. Every login is a potential attack surface. Securing each with strong, phishing-resistant MFA helps close more doors to adversaries.

For support, guidance, or to report phishing activity, contact soc@ren-isac.net.

More Resources

- Microsoft: [Detecting and Mitigating a Multi-Stage AiTM Phishing and BEC Campaign](#)
- Cisco Talos: [State of the Art Phishing: MFA Bypass](#)