Cybercriminals Find New Ways to Get Around Multi-Factor Authentication

Tego Secure IT Solutions | Cloud, Cybersecurity & IT Services > Blog > Security > Cybercriminals Find

Jennifer Vosburgh November 7, 2022 Security

Cybercriminals Find New Ways to Get Around Multi-Factor Authentication

Multi-factor authentication is considered the gold standard for reducing or eliminating phishing schemes. But MFA isn't infallible. As Microsoft has publicly noted, phishing schemes can get around MFA. If you are concerned about protecting your Microsoft 365 access, keep reading.

An MFA Primer

Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA) requires the user to verify their identity on an additional device (such as a mobile phone) before granting access. This extra layer of security ensures only the authorized user can access the account they are logging into. Several providers offer authentication apps that users can use to confirm their identity as they log in. Google, Microsoft, Amazon, and others provide 2FA for users to access their accounts.

Adversary-in-the-Middle Phishing Techniques

These large-scale phishing schemes have already impacted Google users. Victims fall prey by clicking on malicious links or attachments that pick up passwords and cookies and store them. Cybercriminals use the stored credentials to log in to the victim's email on their behalf and delete traces of their malicious activity to remain undetected and perform various intrusion activities, such as sending out additional phishing emails to internal users from the compromised email account.

To guard against this, educate your staff on phishing schemes and use password managers that will only autofill credentials if there is an exact match to the URL (slightly different URLs are one of the ways cybercriminals trick employees). We outline several other options for dealing with phishing schemes here.

Multi-factor Authentication Fatigue Attacks

In addition to being able to bypass MFA, cybercriminals are also coming up with attacks that leverage MFA, according to Rubrik, a Tego data security partner. Recently, Cisco was targeted by a ransomware group, and the malicious actors gained access to Cisco's environment and information.

One of the methods they used as part of their attack was MFA fatigue. MFA fatigue occurs when attackers continuously send a high volume of MFA push requests to the user's mobile device in hopes that they'll accept the request by accident or silence the notifications. Attackers can then gain access to a user's account, enroll new devices for MFA, and gain further privileges within an organization's environment, intruding into the network and accessing sensitive information.

Setting push request limits and educating staff about fatigue attacks is critical. It's also important to have a quick and easy way for employees to notify IT staff so they can report zealous MFA push requests.

The Takeaway: Empower Your Users with Security Awareness Training

Your users are your biggest threat and your greatest asset. Regular security awareness training allows you to educate your users on your organization's security policies and procedures. Security awareness training helps to build a culture of security within your company.

Tego's approach is to make security training engaging and even fun. The training addresses how not to be a victim and discusses how to protect sensitive information, create strong passwords, and the importance of locking your workstation.

Tego can also administer a series of phishing tests as part of our security awareness training. These tests are designed to determine if your users can recognize a phishing attempt or if they would click on a malicious link. Test results are shared and discussed with your administrator to help users spot sophisticated phishing emails.

Contact us today to schedule security awareness training for your organization.

Tags: Backup Cybersecurity Data Retention

Previous Post

Next Post

Search

Recent Posts

» Backup and DR Are Not the Same: What Every CIO Should Know

- » AI in the Data Center: Predictive Maintenance, Capacity Planning and Automated Optimization
- » Shared Responsibility in the Cloud: What CMMC Requires vs. What Cloud Providers Actually Cover
- » How AI Reduces False Positives and SOC Alert Fatigue (And Why Your Analysts Will Thank You)
- » Tego Selected for Cisco NCDIT ITS-400277 Prime Contract Under NC Statewide IT Contract 204X

Recent Comments

No comments to show.

Categories

- » AI
- » Awards
- » Blog
- » Cloud
- » Compliance
- » Cybersecurity
- » Data Privacy
- » Engineering
- » Enterprise Managed Services
- » Environments
- » Expertise
- » IT Infrastructure, Networking, and Security
- » IT Residencies

- IT Service
- News
- Professional Services
- Research
- Security
- Software

Get In Touch

Contact Us →

About Us

Tego is an IT consultancy specializing in custom solutions for data centers, cloud infrastructure, and cybersecurity. With decades of experience, Tego is known for delivering tailored, future-ready IT strategies.

info@tegodata.com
919-792-1741

Solutions

Enterprise Managed Services
IT Infrastructure
Scalable Cloud Solutions
Professional Services
Security, Audit, and Compliance

Who We Serve

Commercial
Enterprise
SLED

Resources

Blog
IT Maturity Assessment
Cloud Assessment Questionnaire

CMMC Discovery Assessment

Tradeshows and Events

FAQ

Contact Us

Privacy Policy • Terms & Conditions