Evolving Threats to Multi-Factor Authentication

Zackary Dowling

July 10, 2025

Agenda

- Introduction
- MFA Bypassing Techniques
- Prevention Techniques
- Questions

RAVEN

Zackary Dowling

Managing Director, Incident Response

About

Zack is a Digital Forensics and Incident Response professional with over 5 years of experience working in Information Security.

As a Managing Director, Zack oversees the Incident Response practice at Raven. He takes charge of the most challenging engagements, while working with customers to get the answers they need. He has led engagements for several enterprise cyber attacks. With a strong technical background, combined with a Master's in Business Administration in Information Technology, he has a well-rounded information security approach and competency communicates both technical and management perspectives.

Previous Focus Areas

Prior to Raven, Zack worked in Incident Response consulting for both a large consulting firm and an Insurance agency. Zack's career in Cybersecurity began with the Massachusetts State Police Cyber Crimes and Digital Forensics Unit.

Passion for Security

Passionate about responding to complex incident response investigations, and brings experience, knowledge and empathy when guiding customers through stressful cyber incidents.

- Holds an Associate's Degree in Criminal Justice, a Bachelor's Degree in Cybersecurity and Networking, and a Master's of Business Administration degree in Information Technology
- Holds the GIAC GCFE, GCFA, GCPN and Microsoft AZ-900 and SC-900 certifications.

RAVEN

MFA Bypassing Techniques

MFA is good, but good enough?

RAVEN

Social Engineering

“Social engineering is a manipulation tactic that exploits human error to steal data, spread malware, or access systems. These ‘human hacking’ attacks can occur online, in person, or through other interactions.”

– Kaspersky

Authority

Intimidation

“Hi, I’m from your IT department – there’s an urgent issue with your account, and I need your login credentials to fix it.”

Consensus

Scarcity

Familiarity

“Your bank account is locked. Click here to verify your identity: **hacker.com**”

Trust

Urgency

A fraudulent site designed to look like a legitimate login page, tricking users into entering their credentials.

RAVEN

MFA Fatigue

How it works?

- Credential stuffing + weak passwords
- **Binary** MFA method bombardment (Push, Call, Text)
- User **accident** or **frustration** enabling access

What to look for?

- Unexpected MFA calls/prompts

SIM Swapping

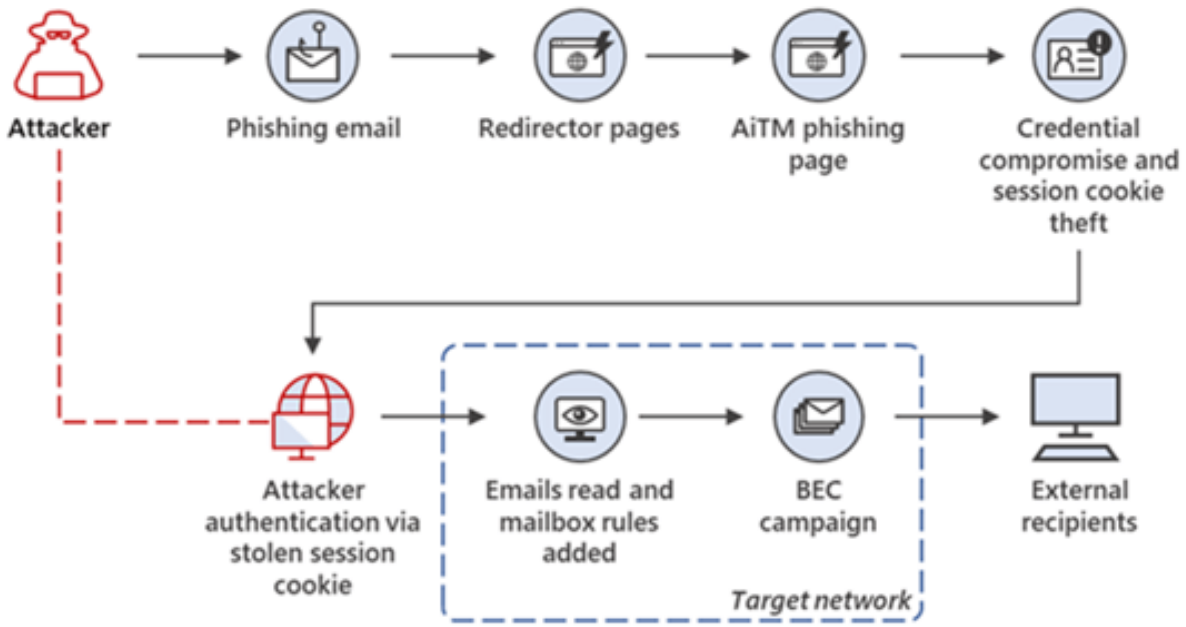
How it works?

- Social engineering of cellular company
- **YOUR** phone number transfers to attacker phone
- Attacker receives Phone or SMS MFA intended for **your** phone number

What to look for?

- Not receiving expected calls or texts

Adversary-in-the-Middle (AiTM)



How it works?

- Attacker controlled website
- **Mimics** login page
- Authentication token captured
- Impersonation of user

What to look for?

- Unfamiliar website URL when logging into a site

login.microsoftonline.com vs. attacker-badsite.com

Fortifying the Weakest Link

What’s the patch for social engineering?

RAVEN

Actionable Strategies to Prevent MFA Bypass

Smart User Behaviors

- Use strong, unique passwords
- Don’t reuse passwords – ever
- Decline unexpected MFA prompts
- Never enter credentials from links or attachments

Modern Authentication Methods

- Adopt phishing-resistant MFA
  - FIDO2
  - WebAuthn
- Avoid binary Yes/No MFA when possible
- Avoid SMS-based one-time codes when possible

Security Controls & Policy

- Enforce Conditional Access
  - Device compliance
  - Geo restrictions
- Tie authentication to verified, compliant devices

Questions?

RAVEN

Thank you!

Emergency Incident Response:

ravenbec.com
support@ravenbec.com

Follow us on LinkedIn!