Phishing Resistant Authentication

By Andrew Regenscheid
National Institute of Standards and Technology
Phishing-Resistant Authentication

Andrew Regenscheid
PIV Technical Lead
NIST Information Technology Laboratory
Disclaimer

Certain commercial entities, equipment, or materials are identified in this presentation in order to describe the concepts adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology (NIST), nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.
Phishing

The USPS package arrived at the warehouse but could not be delivered due to incomplete address information. Please confirm your address in the link.

https://usps.sending-address.com/

(Please reply Y, then exit the text message and open it again to activate the link, or copy the link and open it in your Safari browser).

The USPS team wishes you a wonderful day!
Smishing: Package Tracking Text Scams

Have you received unsolicited mobile text messages with an unfamiliar or strange web link that indicates a USPS delivery requires a response from you? If you never signed up for a USPS tracking request for a specific package, then don't click the link! This type of text message is a scam called smishing.
Cybersecurity Incidents

Data breaches leveraged Phishing attacks\(^1\)

Attacks used involved stolen credentials to gain access\(^1\)

Organizations have faced successful phishing attacks\(^2\)

*Sources:*

\(^1\) 2023 Data Breach Investigations Report, Verizon
\(^2\) 2023 State of the Phish, Proofpoint
Phishing Attacks on Authentication

1. User clicks on link to phishing website
2. Sends password & OTP
3. Attacker uses captured password & OTP at legitimate page
**Authentication** is meant to provide confidence that the returning user is the same that took part in the registration process.

Authentication is accomplished through some combination of three factors:

- **Something you know** – a password
- **Something you have** – one-time passcode (OTP) sent to a device, a USB security key
- **Something you are** – an image of your face or your fingerprint
## Multi-factor Authentication Examples

<table>
<thead>
<tr>
<th>SMS OTP</th>
<th>OTP Apps</th>
<th>Push Authentication</th>
<th>Security Keys</th>
<th>Cryptographic Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>A code that is texted or delivered via audio</td>
<td>App that generates timebound codes</td>
<td>App that sends approval requests to a user</td>
<td>Key for authentication stored on a device</td>
<td>Key for authentication stored through software</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Examples</strong></th>
<th><strong>The Good</strong></th>
<th><strong>The Bad</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>“your verification code is 1234. Don’t share this with anyone else!”</td>
<td>- Anyone with a phone can use it!&lt;br&gt;- Easy to use&lt;br&gt;- SIM Swap protection&lt;br&gt;- Can be done offline</td>
<td>- Highly phishable&lt;br&gt;- Connection required&lt;br&gt;- SIM Swap&lt;br&gt;- Network attacks&lt;br&gt;- Carrier trust reliance</td>
</tr>
<tr>
<td>Google &amp; Microsoft Authenticators</td>
<td>- Easy to use&lt;br&gt;- SIM Swap protection&lt;br&gt;- Some phishing protection</td>
<td>- Highly phishable&lt;br&gt;- App required&lt;br&gt;- Smart phone required&lt;br&gt;- Connection required&lt;br&gt;- App required&lt;br&gt;- User vigilance required&lt;br&gt;- “MFA exhaustion”</td>
</tr>
<tr>
<td>“Press ‘approve’ if you are attempting to access…”</td>
<td>- Easy to use</td>
<td>- Another “thing”&lt;br&gt;- Expensive</td>
</tr>
<tr>
<td>Yubikey, Google Titan, PIV Cards</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### The Good
- Anyone with a phone can use it!
- Easy to use
- SIM Swap protection
- Can be done offline
- Highly secure
- Phishing resistant
- Local MFA option
- Biometric unlock option
- Biometric unlock option

### The Bad
- Highly phishable
- Connection required
- SIM Swap
- Network attacks
- Carrier trust reliance
- Expensive
- Smart device required
- Not user friendly
- Limited market availability
Increased sophistication in phishing attacks as MFA adoption has grown

Steal static authenticators, e.g., passwords

Relay dynamic authenticators, e.g., OTP

Phishing resistant authentication methods address threat vectors:
- Block impersonated websites from capturing authentication data
- Stop Attacker-in-the-Middle from capturing and relaying authentication data from the user to the legitimate website
- Prevent replay attacks that reuse stolen authentication data
- Avoid user entry of secrets that will be sent over the internet

OMB M-22-09 requires federal agencies to offer a phishing-resistant authentication option to public users
Phishing Resistant Methods

**Channel Binding**—*e.g., PKI Certificates with Client-Authenticated TLS*
- Authentication bound to TLS session between client/server
- Strong security properties mitigating web vulnerabilities/attacks
- Requires PKI and user certificates

**Verifier Name Binding**—*e.g., WebAuthn/FIDO2*
- Authentication bound to web origin/domain
- Prevents relay attacks by lookalike/phishing web sites
- Authenticators embedded in platforms or as standalone tokens
Cryptographic authentication using credentials issued to users from trusted Certificate Authorities

**Examples:** Credentials may be stored on:
- Smart Cards—PIV, CAC, PIV-I
- Embedded in device/OS key stores
- USB tokens

Strong two-way authentication between the user and the website or application prevents phishing and relay attacks

Widely used within the federal government

Significant infrastructure required to deploy and use, limiting commercial use
WebAuthn, FIDO and Passkeys

- Cryptographic authentication using public key credentials bound to user accounts
  - Uses website-specific credentials to protect security and privacy
  - Credentials must be created and registered at each website/application

- **Examples:** Credentials may be stored and used on:
  - USB/NFC Security Keys
  - Platform authenticators embedded in mobile devices and PCs

- Resists phishing attacks by:
  - Using website-specific credentials scoped to domain name
  - Browsers will not use legitimate credentials on lookalike phishing sites

- Can register multiple authenticators on each website to mitigate risk of loss
- Commercial support rapidly increasing
NIST Digital Identity Guidelines

• NIST SP 800-63 details the process and technical requirements for Digital Identity

• Four volumes:
  • Base – Digital Identity Model and Risk Management
  • A – Identity Proofing & Enrollment
  • B – Authentication & Lifecycle Management
  • C – Federation & Assertions

• Major draft revision was in December 2022
**SP 800-63B Overview**

**Scope:** Authentication and Lifecycle Management
- Authenticators to authenticate *subjects* to *relying parties*.
- Authentication processes and protocols used by *verifiers*.
- Lifecycle:
  - Authenticator Selection and equity considerations
  - Authenticator Binding/Issuance
  - Session management
  - Account recovery

**Authentication Assurance Levels**

<table>
<thead>
<tr>
<th>AAL1</th>
<th>Single-factor authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAL2</td>
<td>Multifactor authentication</td>
</tr>
<tr>
<td></td>
<td>Supports implementation of EO 14028 and EO 13681 for MFA</td>
</tr>
<tr>
<td>AAL3</td>
<td>Hardware-based, cryptographic multifactor authentication</td>
</tr>
<tr>
<td></td>
<td>Phishing resistant in support of OMB M-22-09</td>
</tr>
<tr>
<td></td>
<td>Supported by PIV at federal agencies, consistent with HSPD-12</td>
</tr>
</tbody>
</table>
Additional Resources

NIST Guidelines

• NIST SP 800-64-4, Initial Public Draft, Digital Identity Guidelines, December 2022
• NIST SP 800-63-3, Digital Identity Guidelines, June 2017

NIST Informative Materials:

• Blog: Phishing Resistance – Protecting the Keys to Your Kingdom
• Video: Protecting Your Small Business: Phishing
• Video: Introducing Phish Scale

CISA Guidance:

• Implementing Phishing Resistant MFA
Questions

Andrew Regenscheid, PIV Technical Lead
NIST Information Technology Lab
Andrew.Regenscheid@NIST.gov