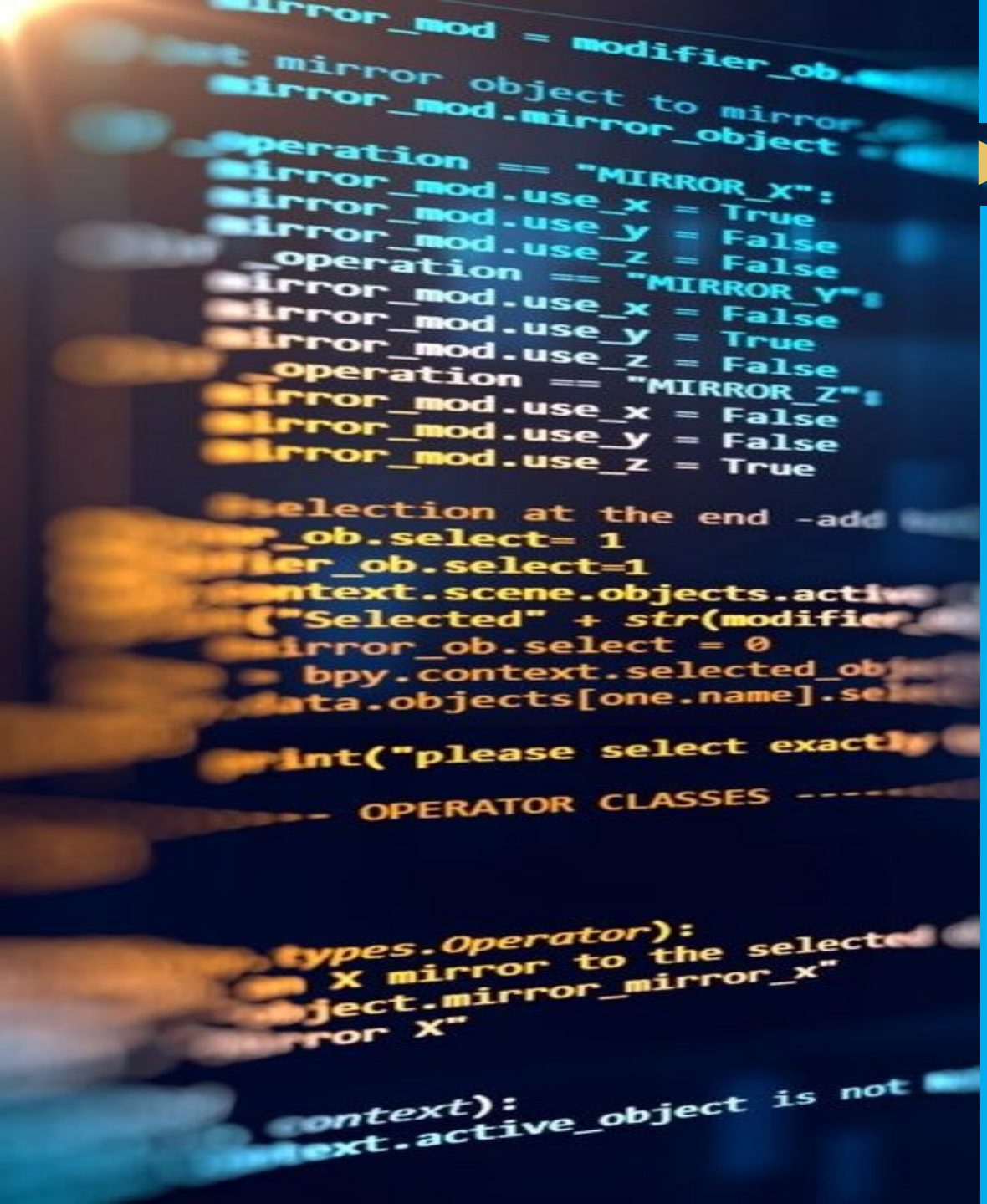


AN OFFERING IN THE BLUE CYBER SERIES

Phishing Resistant Authentication

By Andrew Regenscheid

National Institute of Standards and Technology

26 September 2023

BLUE CYBER EDUCATION SERIES

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Phishing-Resistant Authentication

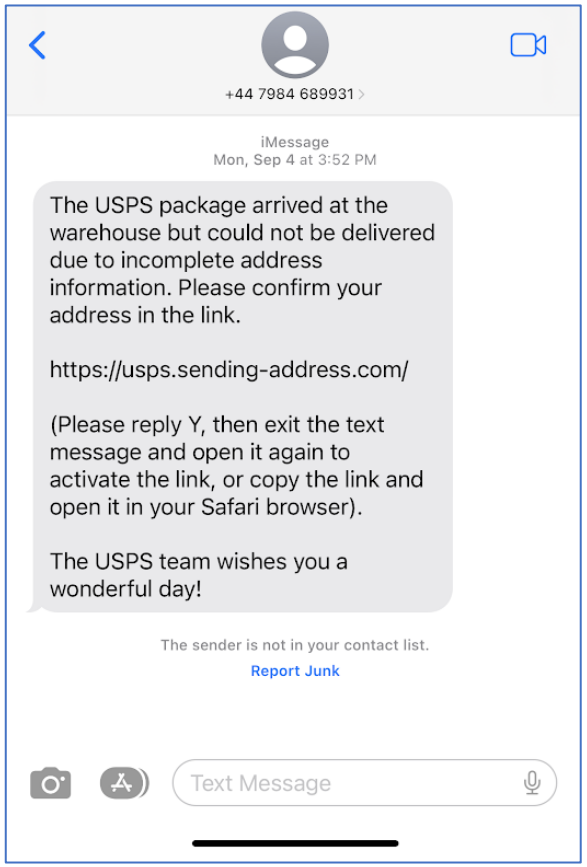
Andrew Regenscheid
PIV Technical Lead
NIST Information Technology Laboratory

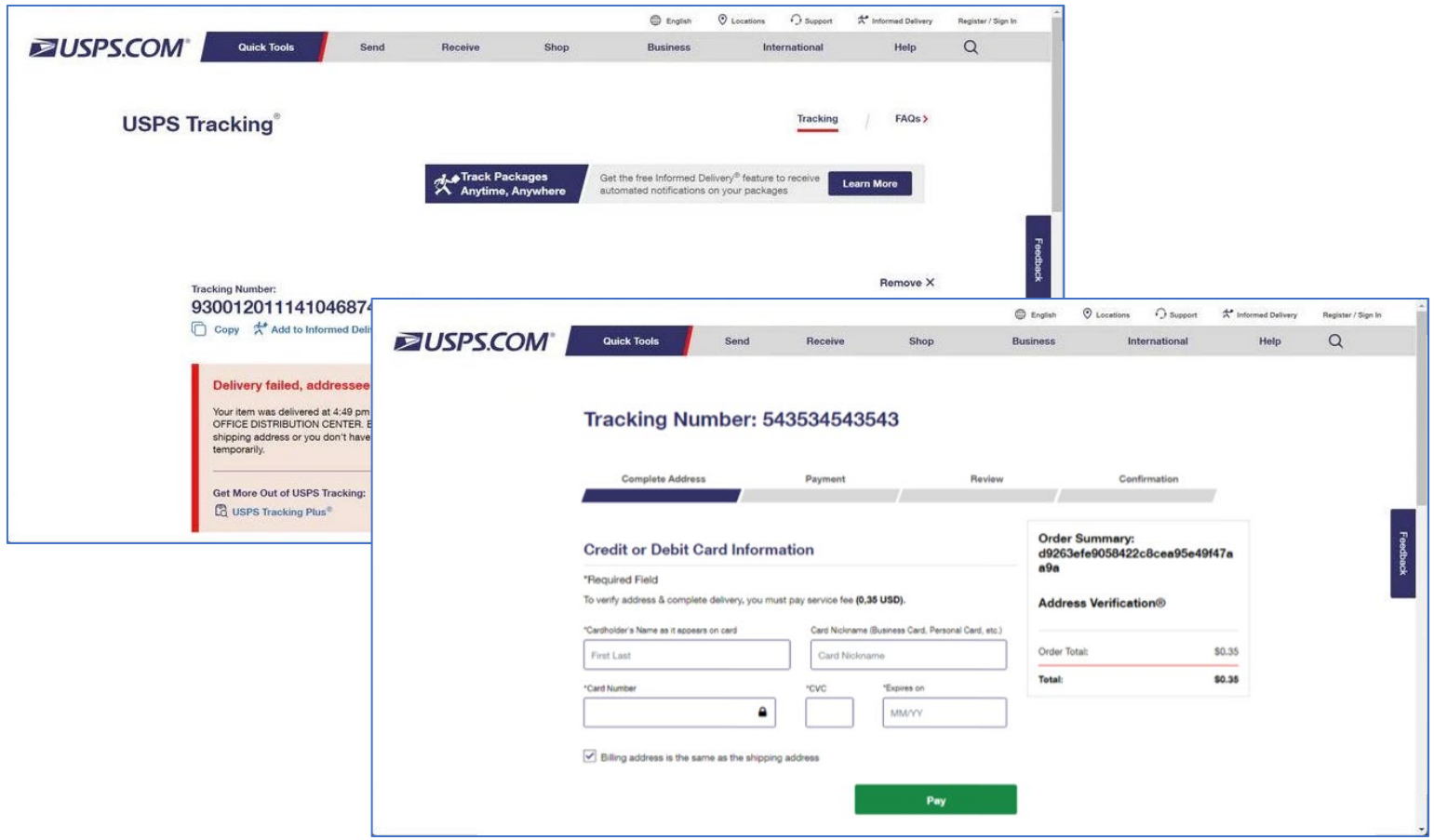
26 September 2023

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


+44 7984 689931
iMessage
Mon, Sep 4 at 3:52 PM
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!
The sender is not in your contact list.
Report Junk
Text Message


USPS.COM
Quick Tools
Send
Receive
Shop
Business
International
Help
USPS Tracking
Tracking
FAQs
Track Packages Anytime, Anywhere
Get the free Informed Delivery feature to receive automated notifications on your packages
Learn More
Feedback
Remove
Tracking Number:
Delivery failed, addressee
Get More Out of USPS Tracking:
USPS Tracking Plus
Tracking Number: 543534543543
Complete Address
Payment
Review
Confirmation
Credit or Debit Card Information
*Required Field
To verify address & complete delivery, you must pay service fee (0.35 USD).
*Cardholder's Name as it appears on card
First Last
Card Nickname (Business Card, Personal Card, etc.)
Card Nickname
*Card Number
*CVC
*Expires on
MM/YY
Billing address is the same as the shipping address
Pay
Order Summary:
d9263efe9058422c8cea95e49f47aa9a
Address Verification®
Order Total: $0.35
Total: $0.35

Phishing

UNITED STATES POSTAL INSPECTION SERVICE

ABOUT | CAREERS | TIPS & PREVENTION | NEWS | REPORT

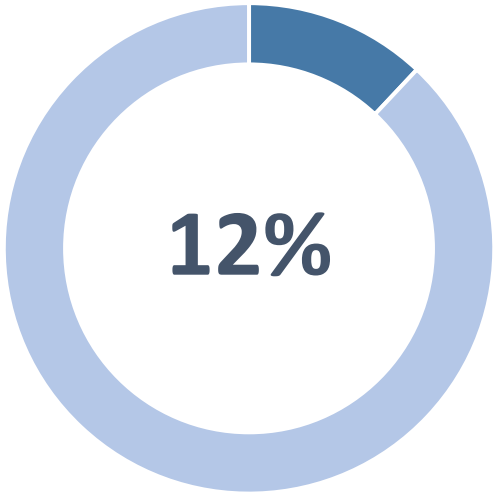
Scam Article

Smishing: Package Tracking Text Scams

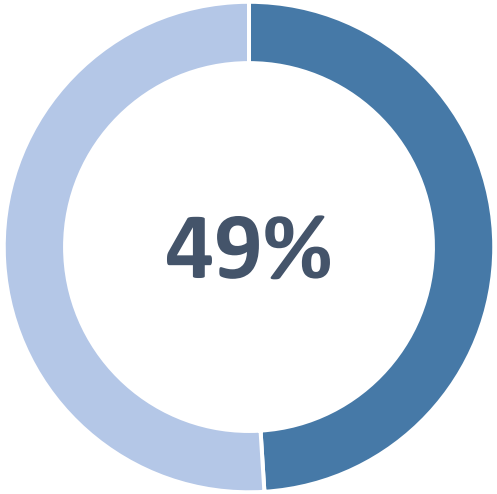
Last updated 03.14.2023 | National

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.

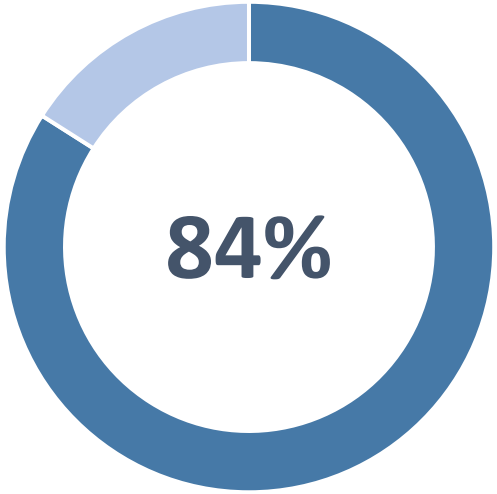
Cybersecurity Incidents



Data breaches leveraged Phishing attacks[1]



Attacks used involved stolen credentials to gain access[1]



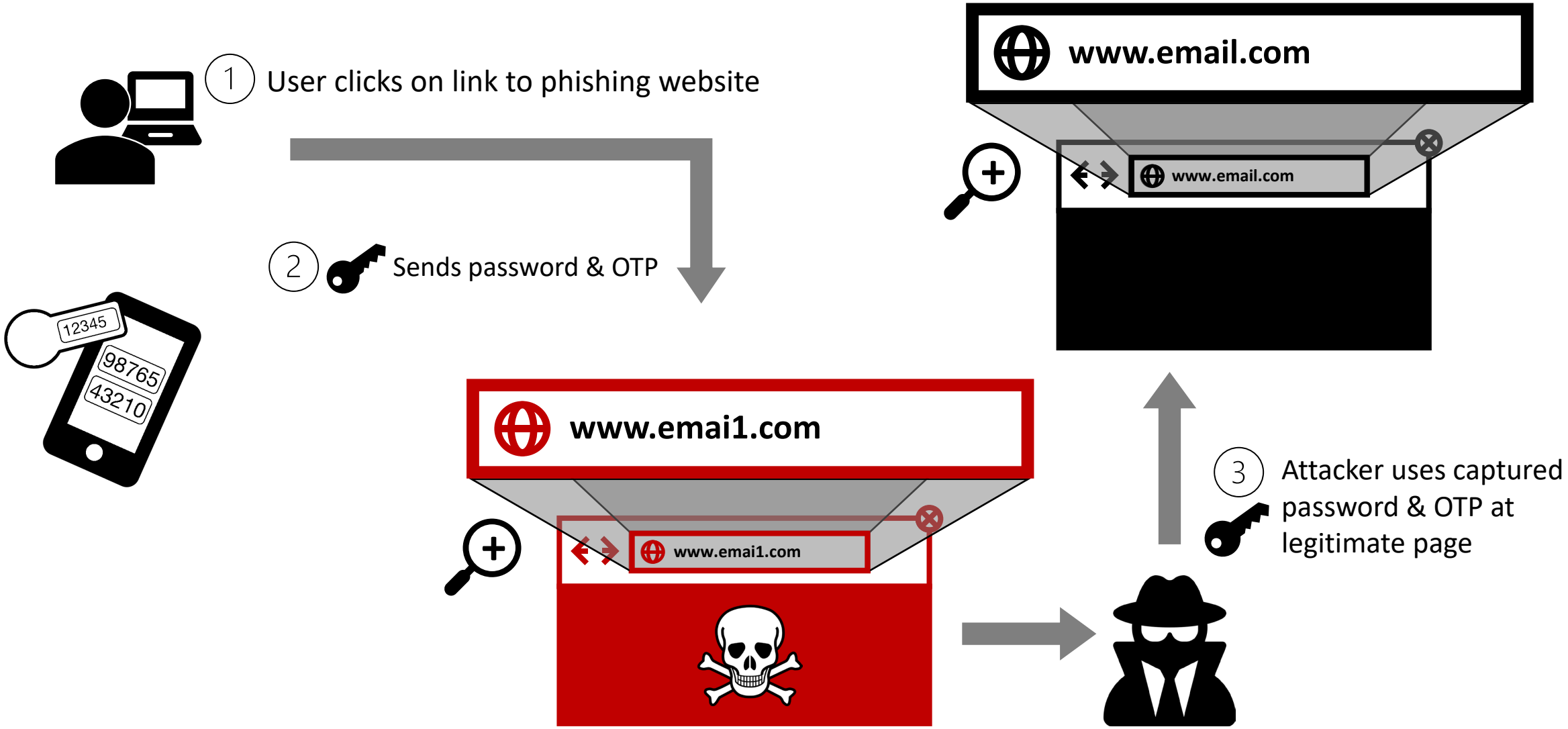
Organizations have faced successful phishing attacks[2]

Sources:

[1] 2023 Data Breach Investigations Report, Verizon

[2] 2023 State of the Phish, Proofpoint

Phishing Attacks on Authentication

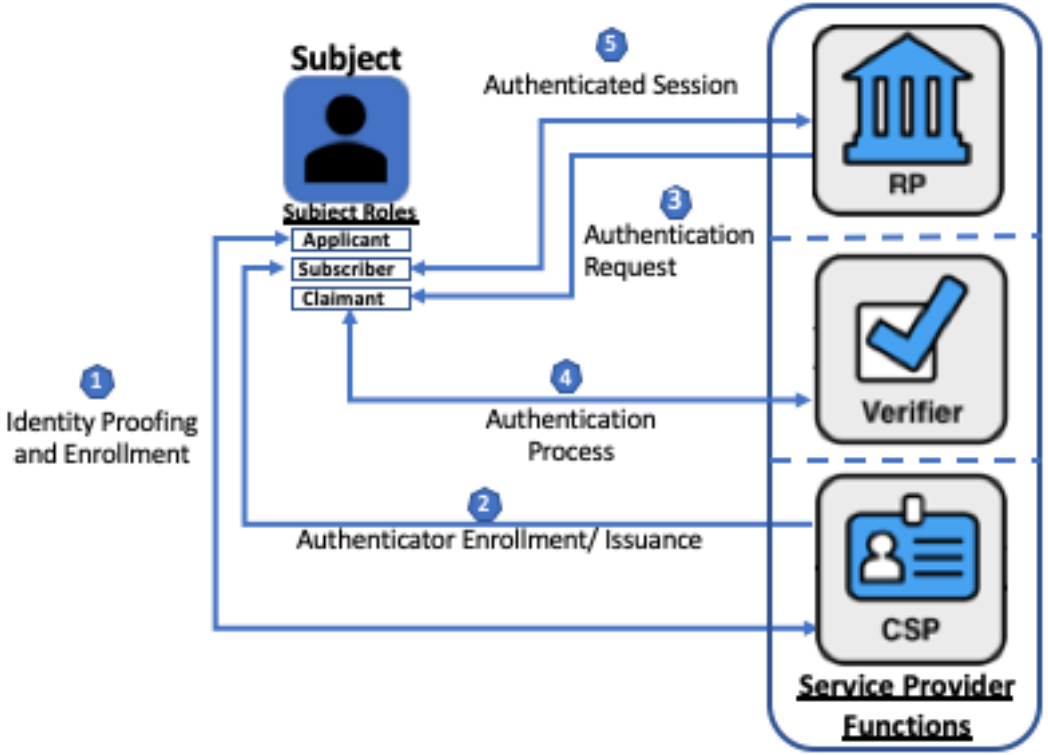


Authentication

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

	SMS OTP A code that is texted or delivered via audio	**OTP Apps** *App that generates timebound codes*	**Push Authentication** *App that sends approval requests to a user*	**Security Keys** *Key for authentication stored on a device*	**Cryptographic Apps** *Key for authentication stored through software*
Examples	"your verification code is 1234. Don't share this with anyone else!"	Google & Microsoft Authenticators	"Press 'approve' if you are attempting to access…"	Yubikey, Google Titan, PIV Cards	FaceID, Windows Hello, passkeys
The Good	➢ Anyone with a phone can use it!	➢ Easy to use ➢ SIM Swap protection ➢ Can be done offline	➢ Easy to use ➢ SIM Swap protection ➢ Some phishing protection	➢ Highly secure ➢ Phishing resistant ➢ Local MFA option ➢ Biometric unlock option	➢ Highly secure ➢ Phishing resistant ➢ "Passwordless" MFA ➢ Biometric unlock option
The Bad	➢ Highly phishable ➢ Connection required ➢ SIM Swap ➢ Network attacks ➢ Carrier trust reliance	➢ Highly phishable ➢ App required ➢ Smart phone required	➢ Connection required ➢ App required ➢ User vigilance required ➢ "MFA exhaustion"	➢ Another "thing" ➢ Expensive	➢ Smart device required ➢ Not user friendly ➢ Limited market availability

Phishing Resistance

Increased sophistication in phishing attacks as MFA adoption has grown

Steal static authenticators, e.g., passwords

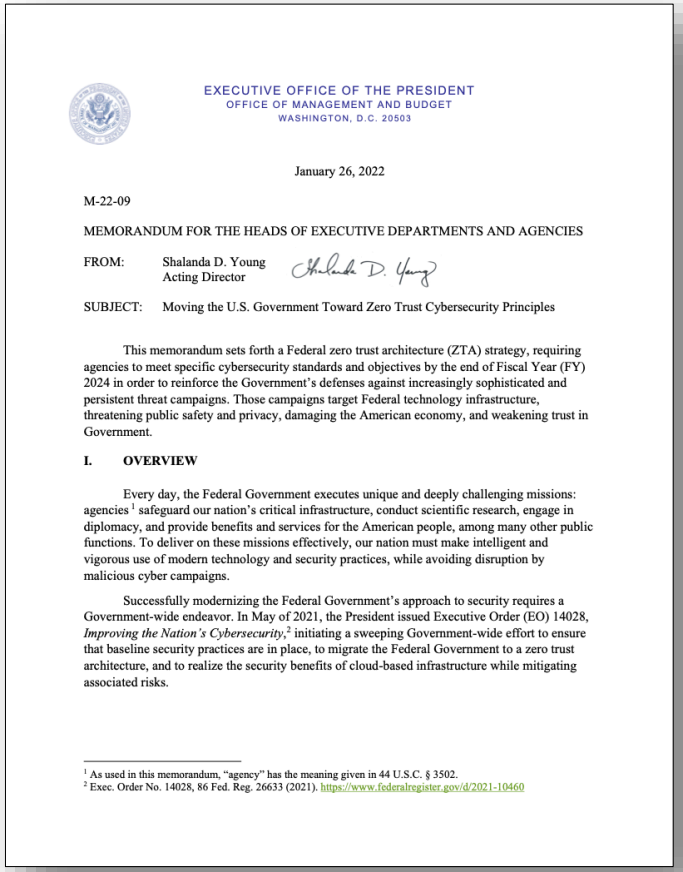
→

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



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

January 26, 2022

M-22-09

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young
Acting Director

SUBJECT: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

This memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. Those campaigns target Federal technology infrastructure, threatening public safety and privacy, damaging the American economy, and weakening trust in Government.

I. OVERVIEW

Every day, the Federal Government executes unique and deeply challenging missions: agencies [1] safeguard our nation's critical infrastructure, conduct scientific research, engage in diplomacy, and provide benefits and services for the American people, among many other public functions. To deliver on these missions effectively, our nation must make intelligent and vigorous use of modern technology and security practices, while avoiding disruption by malicious cyber campaigns.

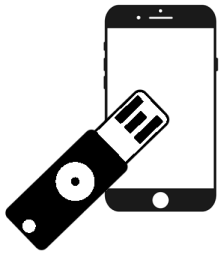
Successfully modernizing the Federal Government's approach to security requires a Government-wide endeavor. In May of 2021, the President issued Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*,[2] initiating a sweeping Government-wide effort to ensure that baseline security practices are in place, to migrate the Federal Government to a zero trust architecture, and to realize the security benefits of cloud-based infrastructure while mitigating associated risks.

[1] As used in this memorandum, "agency" has the meaning given in 44 U.S.C. § 3502.
[2] Exec. Order No. 14028, 86 Fed. Reg. 26633 (2021). https://www.federalregister.gov/d/2021-10460

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 and user certificates

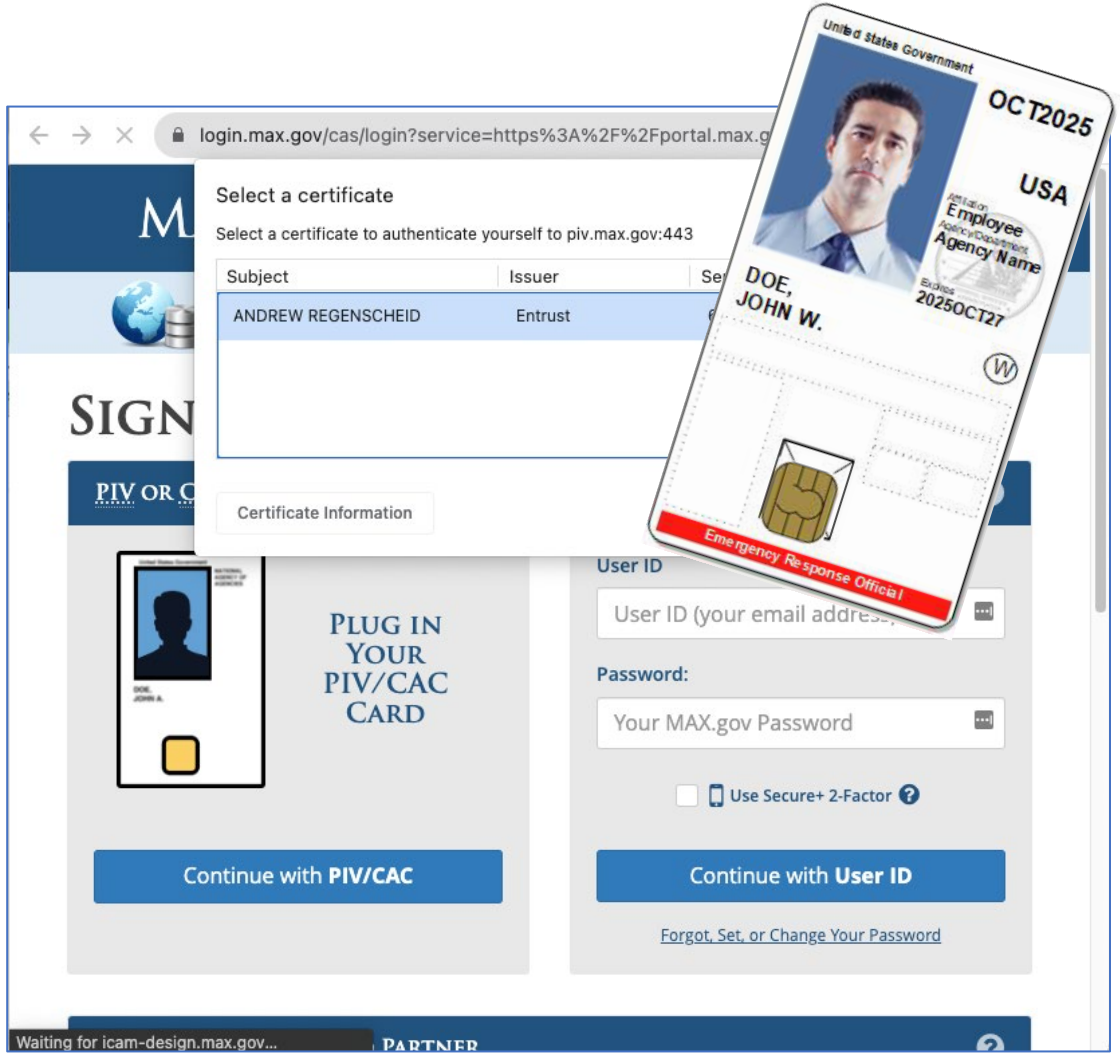


Verifier Name Binding– *e.g., WebAuthn/FIDO2*

- Authentication bound to web origin/domain
- Prevents relay attacks by lookalike/phishing web sites
- Authenticators embedded in platforms or as standalone tokens

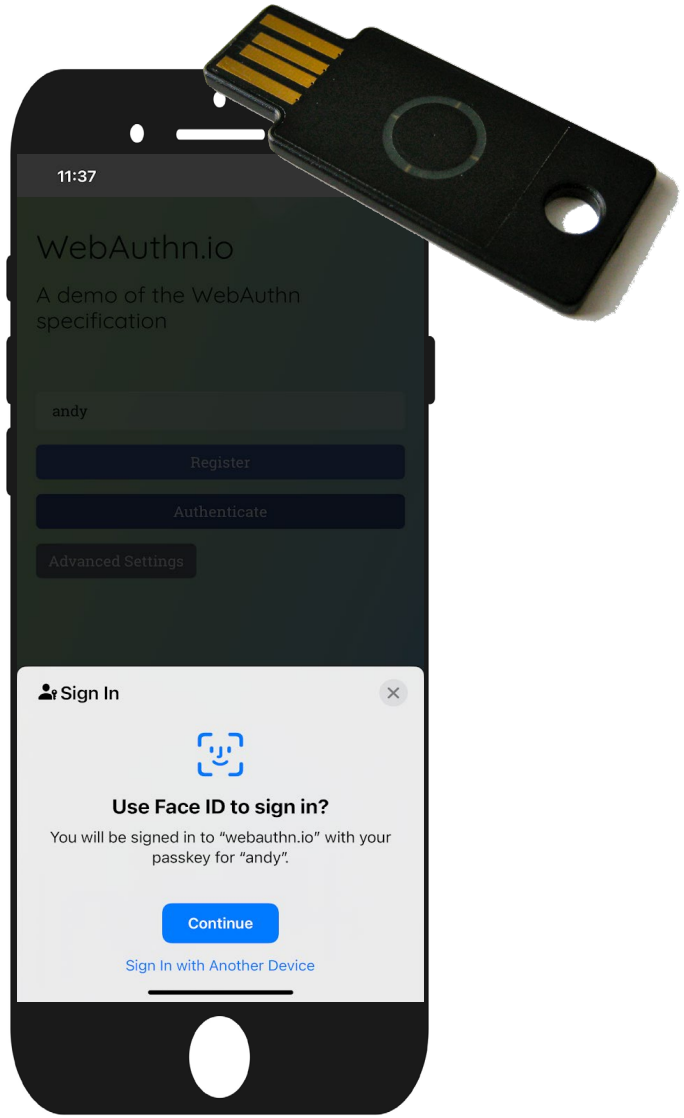
PKI Certificates and Client-Auth TLS

- 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



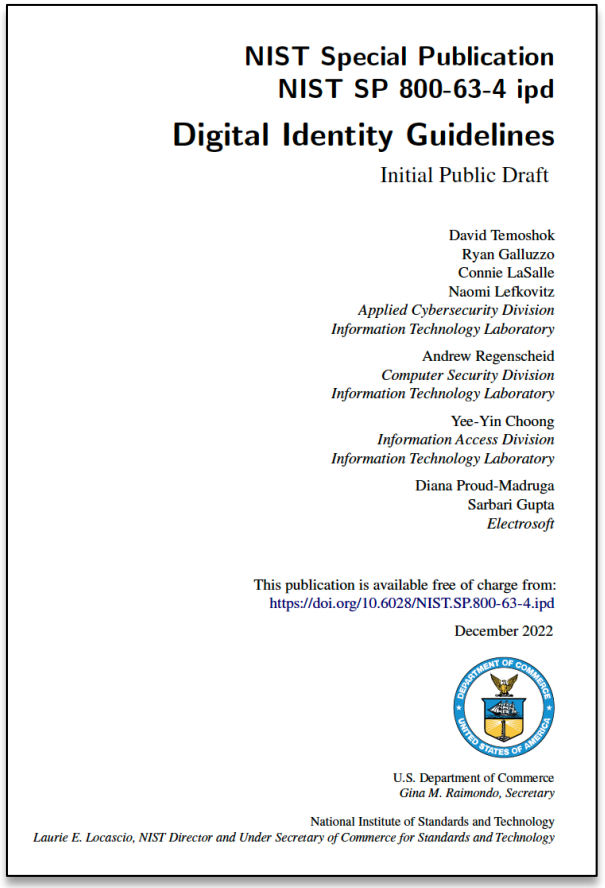
WebAuthn, FIDO and Passkeys

- 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



NIST Special Publication
NIST SP 800-63-4 ipd

Digital Identity Guidelines

Initial Public Draft

David Temoshok
Ryan Galluzzo
Connie LaSalle
Naomi Lefkovitz
Applied Cybersecurity Division
Information Technology Laboratory

Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

Yee-Yin Choong
Information Access Division
Information Technology Laboratory

Diana Proud-Madruga
Sarbari Gupta
Electrosoft

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-4.ipd

December 2022

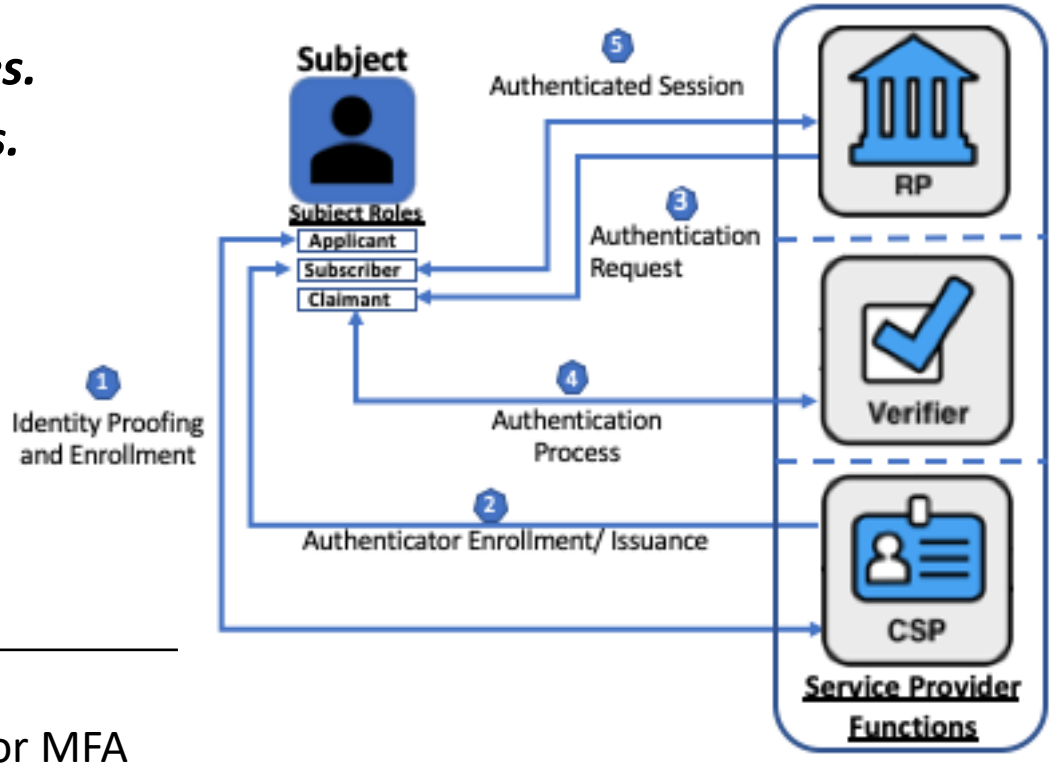
U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

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

AAL1	• Single-factor authentication
AAL2	• Multifactor authentication • Supports implementation of EO 14028 and EO 13681 for MFA
AAL3	• Hardware-based, cryptographic multifactor authentication • Phishing resistant in support of OMB M -22-09 • Supported by PIV at federal agencies, consistent with HSPD-12

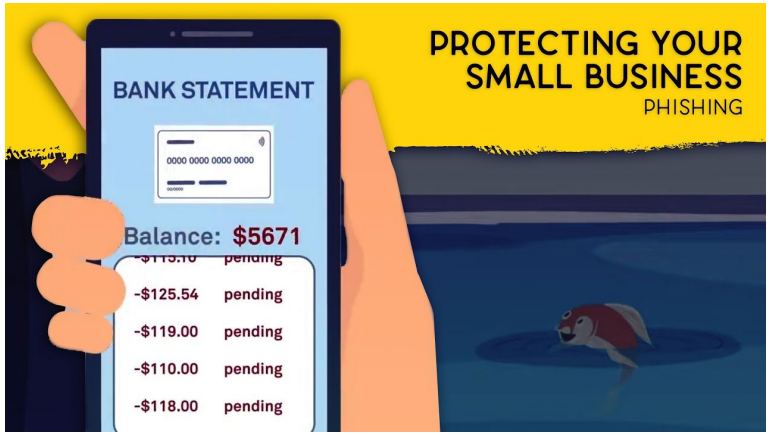
Additional Resources

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