Filet-O-Phish:

What makes phishing-resistant MFA phishing resistant?

Microsoft Most Valuable Professional

Eric Woodruff

Product Technical Specialist
Semperis

Hybrid Identity Protection

Filet-O-Phish

Eric Woodruff

Product Technical Specialist
Semperis

Microsoft Security MVP

ericonidentity.com

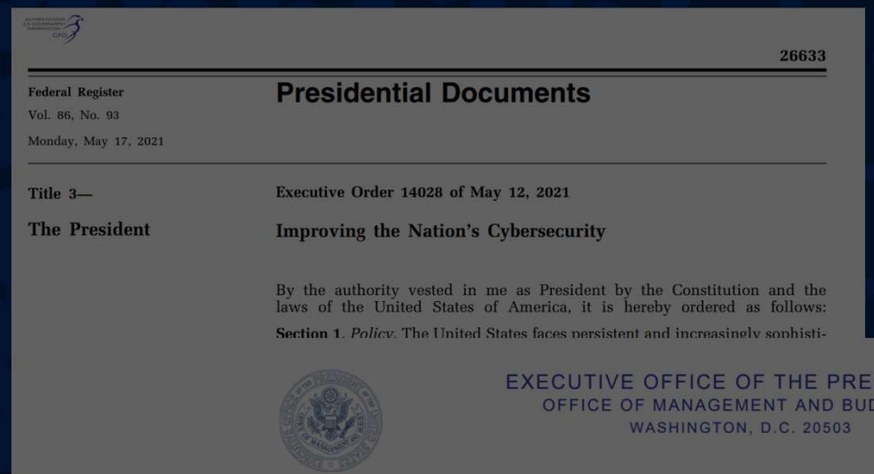
@ericonidentity.com

@msft_hiker

@ericonidentity@infosec.exchange

/in/msfthiker

Hybrid Identity Protection



26633

Federal Register
Vol. 86, No. 93
Monday, May 17, 2021

Presidential Documents

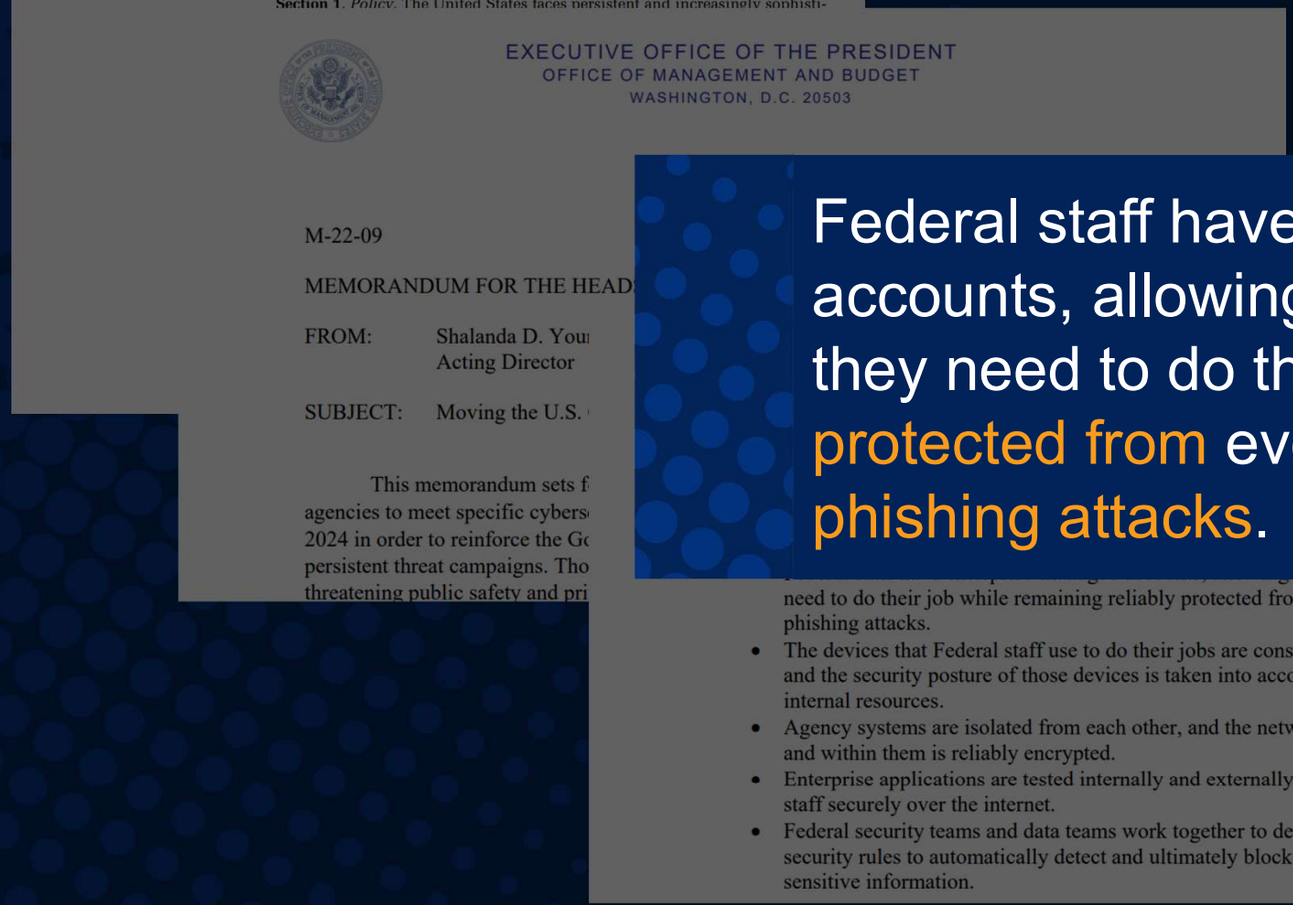
Title 3—
The President

Executive Order 14028 of May 12, 2021

Improving the Nation's Cybersecurity

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. *Policy*. The United States faces persistent and increasingly sophisti-



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

M-22-09

MEMORANDUM FOR THE HEAD

FROM: Shalanda D. You
Acting Director

SUBJECT: Moving the U.S.

This memorandum sets f
agencies to meet specific cybers
2024 in order to reinforce the G
persistent threat campaigns. Tho
threatening public safety and pri

need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.

- The devices that Federal staff use to do their jobs are consistently tracked and monitored, and the security posture of those devices is taken into account when granting access to internal resources.
- Agency systems are isolated from each other, and the network traffic flowing between and within them is reliably encrypted.
- Enterprise applications are tested internally and externally, and can be made available to staff securely over the internet.
- Federal security teams and data teams work together to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.

Federal staff have enterprise-managed accounts, allowing them to access everything they need to do their job while remaining reliably protected from even targeted, sophisticated phishing attacks.

Hybrid Identity Protection

Business Email Compromise (BEC)

35 Million

Annual BEC Attempts[1]

[1]Between April 2022 – April 2023. Microsoft Cyber Signals, May 2023, page 3

Business Email Compromise (BEC)

156,000

Daily BEC Attempts[1]

[1]Between April 2022 – April 2023. Microsoft Cyber Signals, May 2023, page 3

Hybrid Identity Protection

Business Email Compromise (BEC)

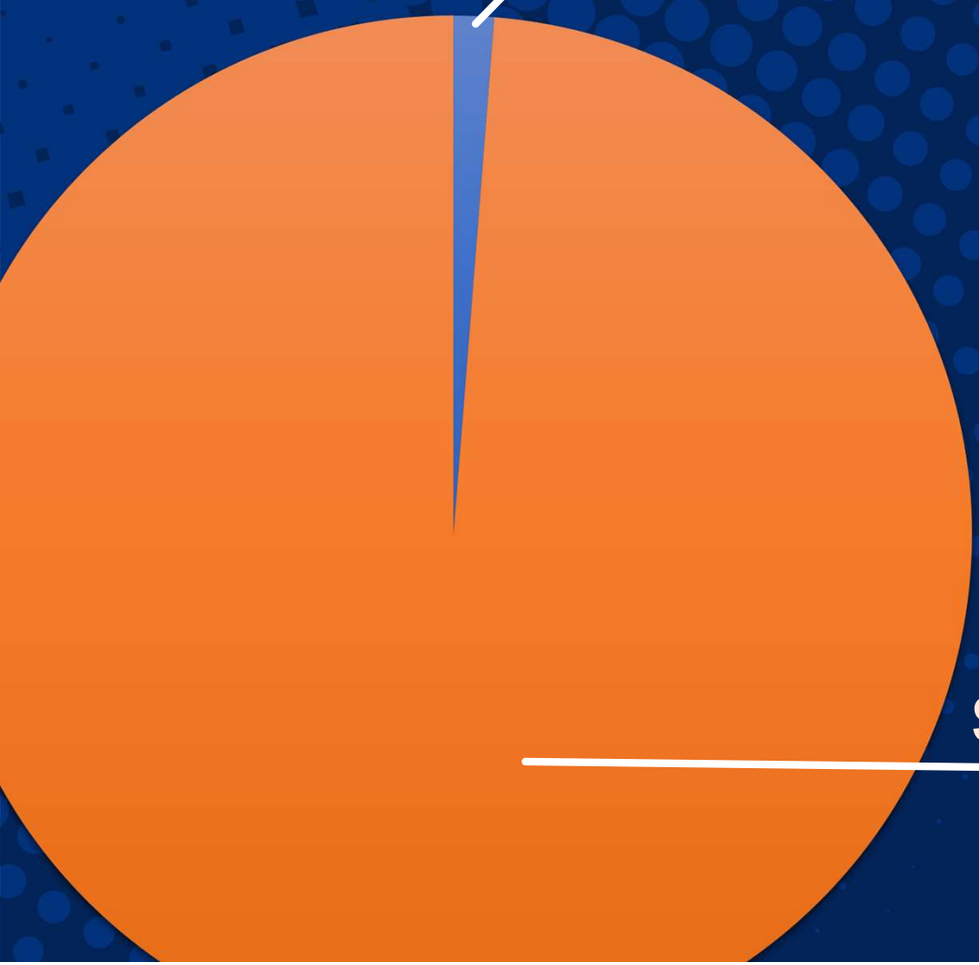
417,678

Phishing URL Takedowns[1]

[1]Between April 2022 – April 2023. Microsoft Cyber Signals, May 2023, page 3

Hybrid Identity Protection

Business Email Compromise (BEC)



$34.3 million USD[1]

Ransomware

FBI IC3 Crime Report 2022
Domestic adjusted losses

$2.7 billion USD[2]

BEC

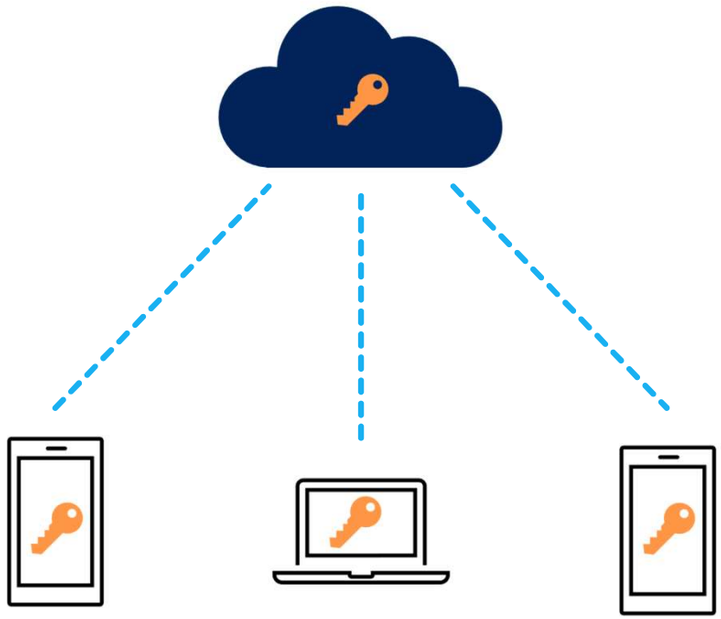
[1]FBI Internet Crime Report 2022, page 13
[2]FBI Internet Crime Report 2022, page 11

Hybrid Identity Protection

Entra ID Authentication Strengths

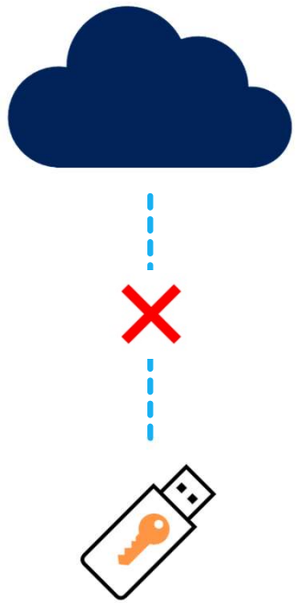
Authentication Method	Satisifes MFA	Passwordless	Phishing-resistant
Device-bound passkey	☑	☑	☑
Windows Hello for Business	☑	☑	☑
Certificate-based authentication (multi-factor)	☑	☑	☑
Microsoft Authenticator Phone Sign-in	☑	☑	✗
Password + MS Authenticator Push Notification	☑	✗	✗
Password + OTP	☑	✗	✗
Temporary Access Pass (TAP)	☑	✗	✗
Password	✗	✗	✗

Passkeys and FIDO2



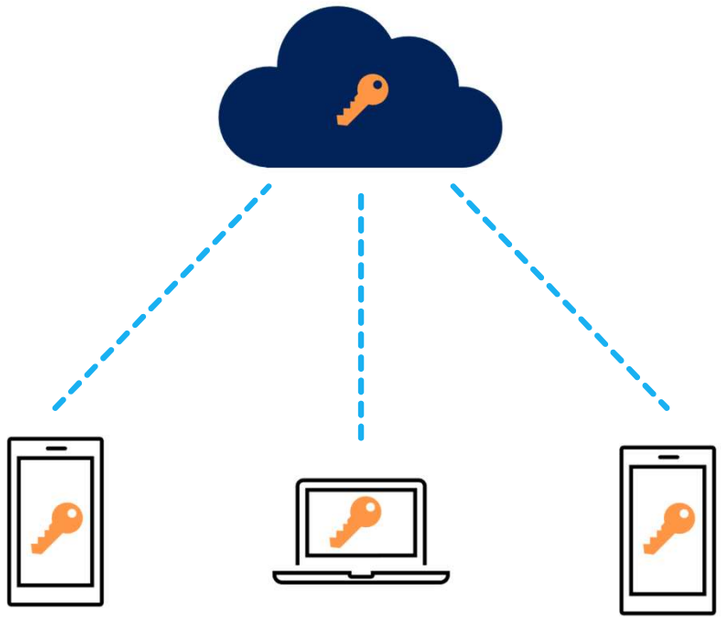
Passkey

Multi-device passkeys



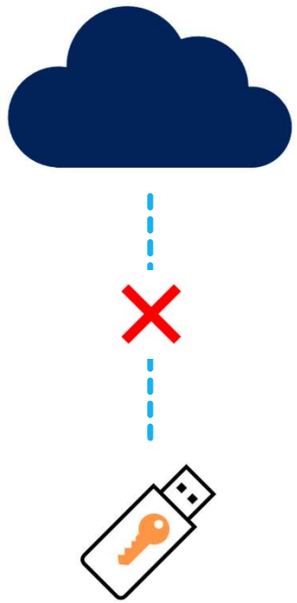
FIDO2 Security Key

Passkeys and FIDO2



Passkey

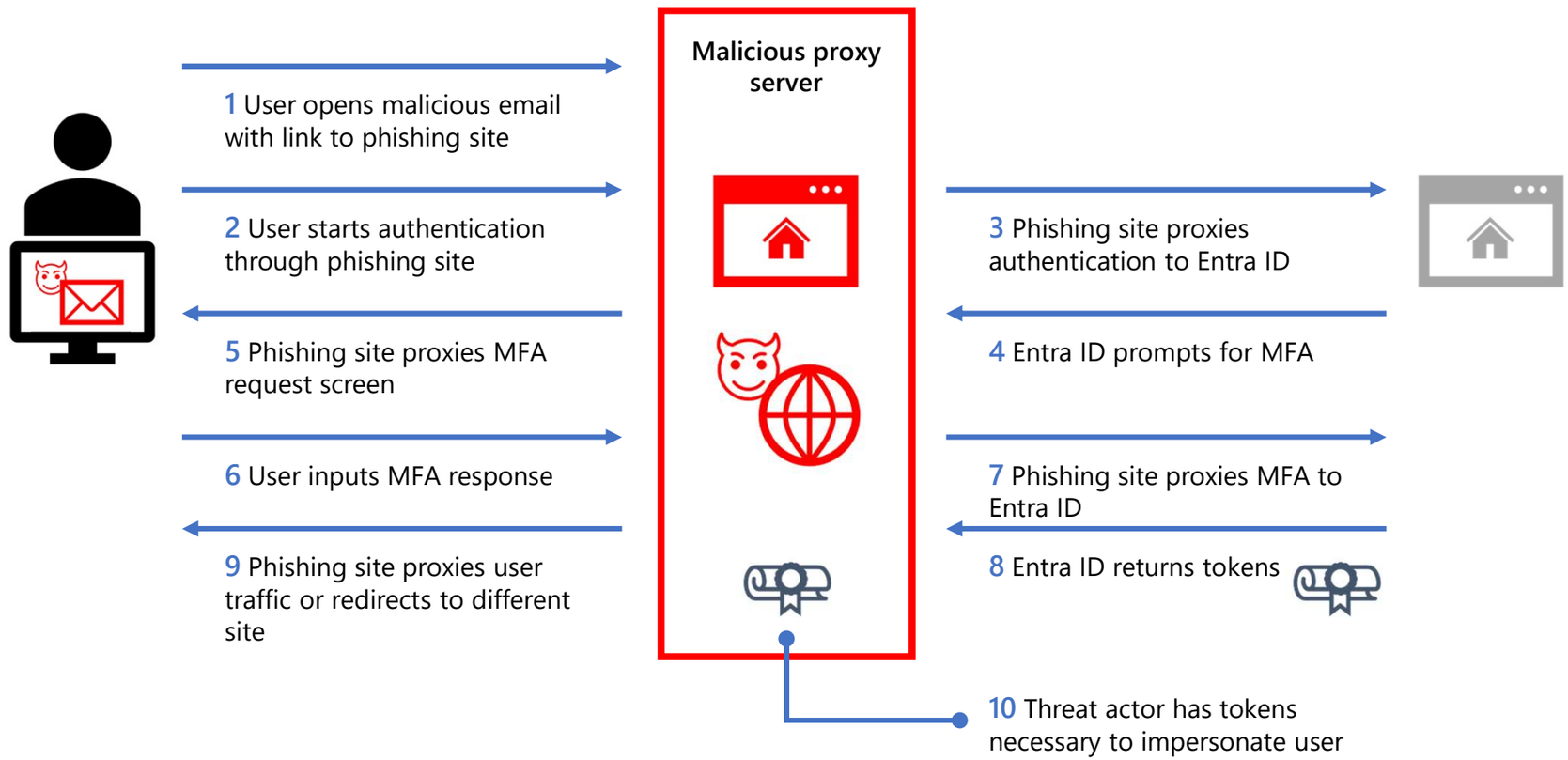
Multi-device passkeys



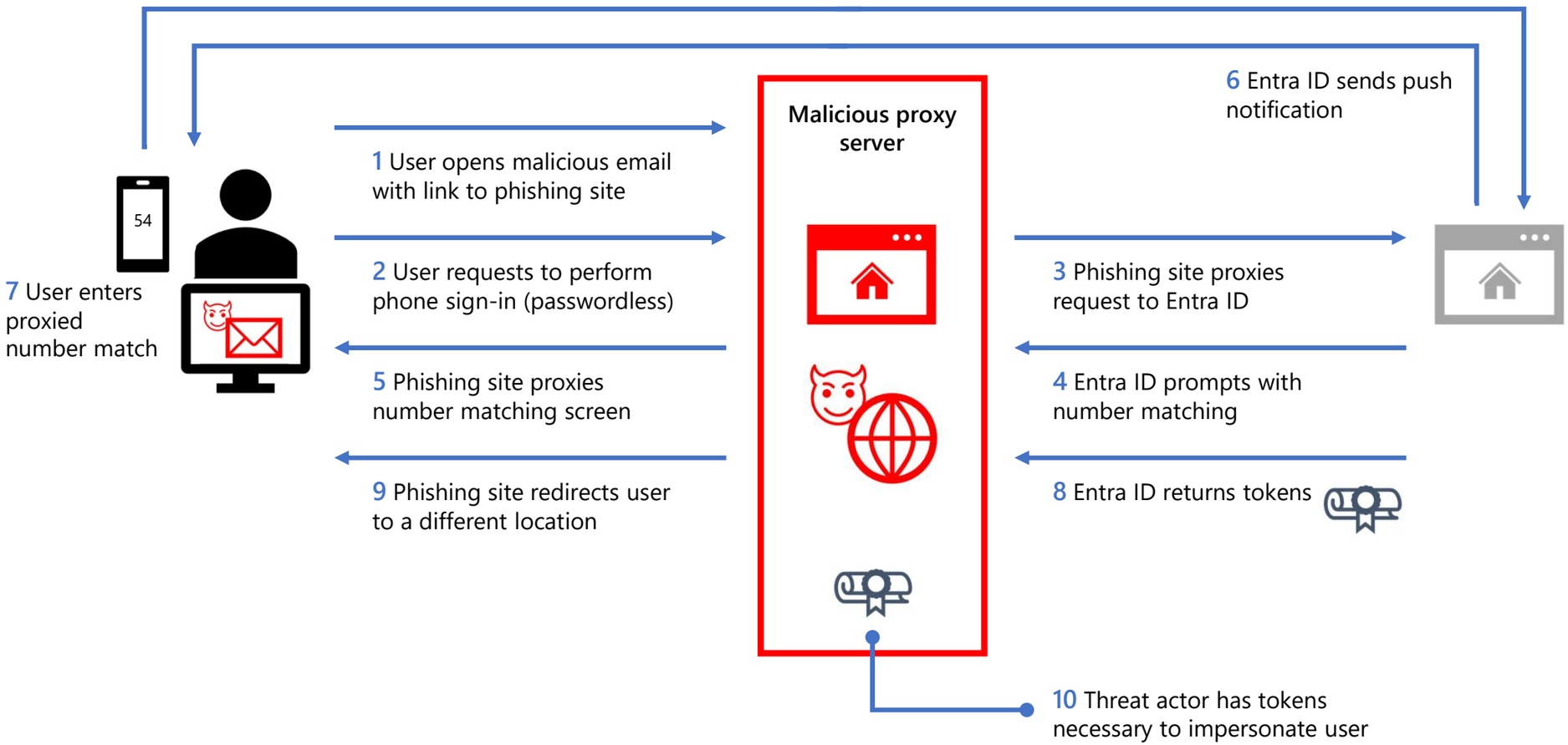
Device-bound passkey

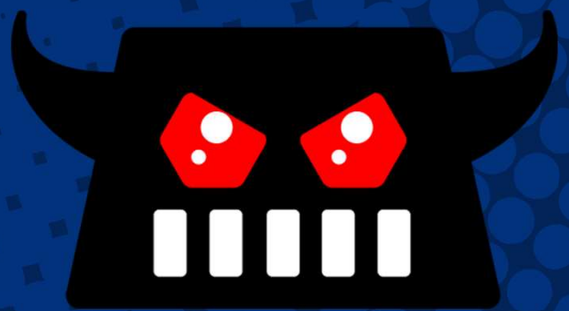
Non-syncable passkeys

Modern Phishing Attack - OTP



Modern Phishing Attack – Phone Sign-in





Evilginx Demonstration

Hybrid Identity Protection

INTERNATIONAL TELECOMMUNICATION UNION

CCITT

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

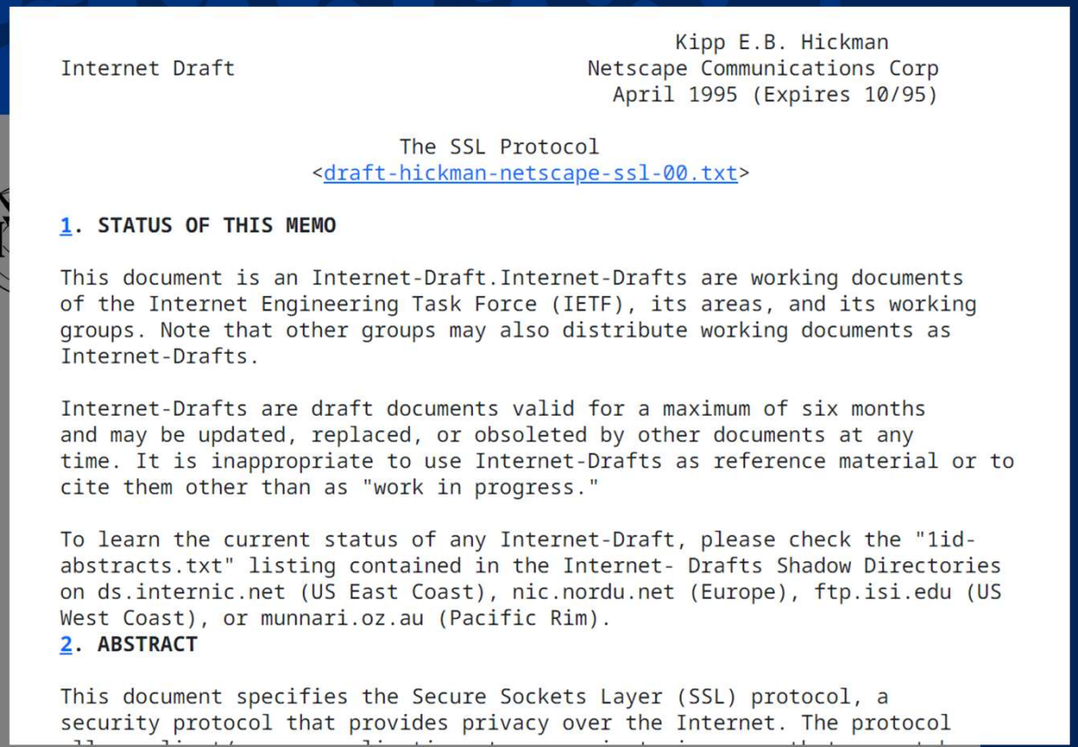
X.509

(11/1988)

SERIES X: DATA COMMUNICATION NETWORKS:
DIRECTORY

THE DIRECTORY – AUTHENTICATION FRAMEWORK

Hybrid Identity Protection



Internet Draft

Kipp E.B. Hickman
Netscape Communications Corp
April 1995 (Expires 10/95)

The SSL Protocol
<draft-hickman-netscape-ssl-00.txt>

1. STATUS OF THIS MEMO

This document is an Internet-Draft.Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

To learn the current status of any Internet-Draft, please check the "1id-abstracts.txt" listing contained in the Internet- Drafts Shadow Directories on ds.internic.net (US East Coast), nic.nordu.net (Europe), ftp.isi.edu (US West Coast), or munnari.oz.au (Pacific Rim).

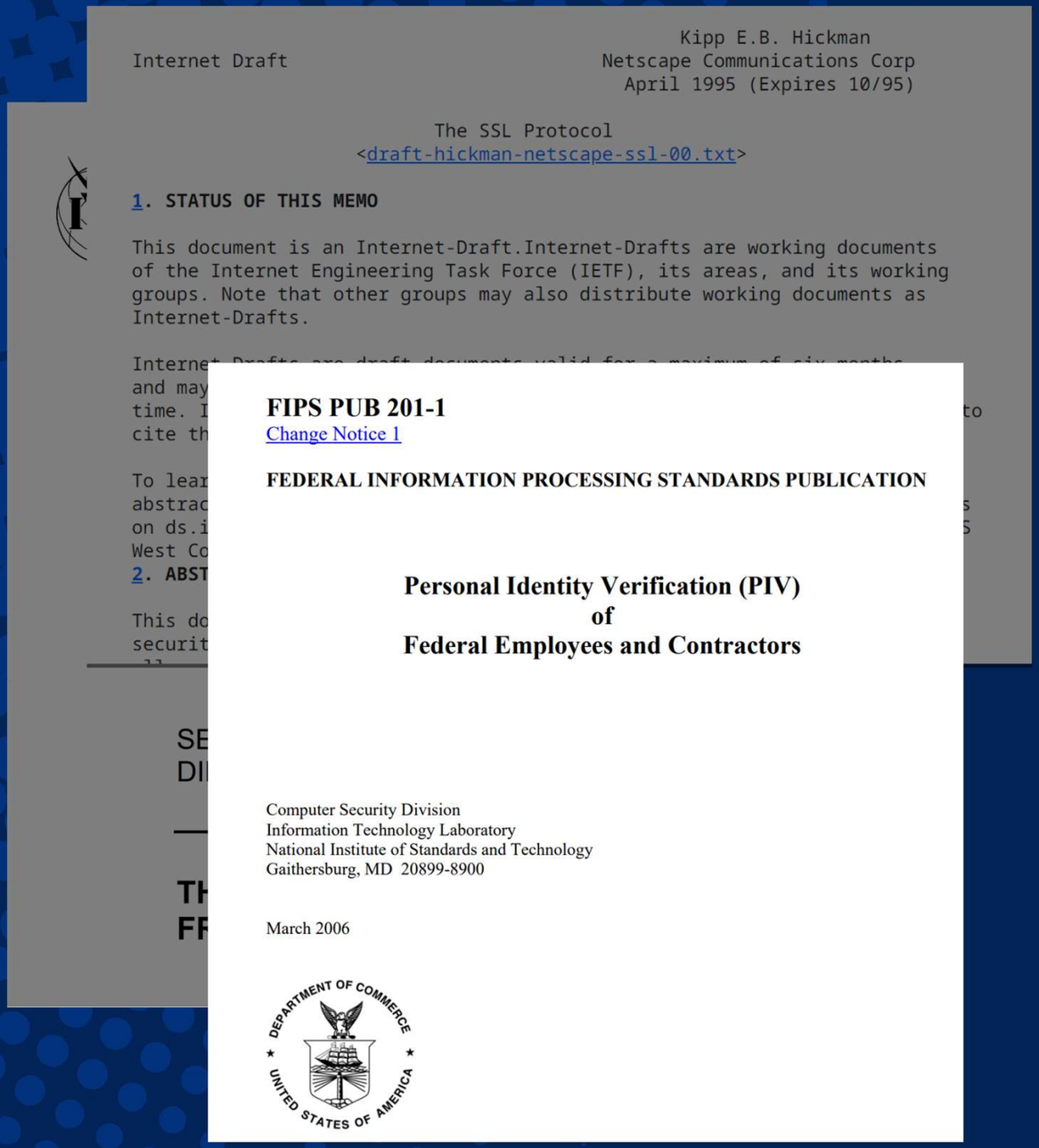
2. ABSTRACT

This document specifies the Secure Sockets Layer (SSL) protocol, a security protocol that provides privacy over the Internet. The protocol

SERIES X: DATA COMMUNICATION NETWORKS: DIRECTORY

THE DIRECTORY – AUTHENTICATION FRAMEWORK

TLS



Internet Draft

Kipp E.B. Hickman
Netscape Communications Corp
April 1995 (Expires 10/95)

The SSL Protocol
<draft-hickman-netscape-ssl-00.txt>

1. STATUS OF THIS MEMO

This document is an Internet-Draft.Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

FIPS PUB 201-1
Change Notice 1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV)
of
Federal Employees and Contractors

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

March 2006

DEPARTMENT OF COMMERCE
UNITED STATES OF AMERICA

PIV

Hybrid Identity Protection

W3C Working Draft

Web Authentication: A Web API for accessing scoped credentials

W3C First Public Working Draft, 31 May 2016

This version:
http://www.w3.org/TR/2016/WD-webauthn-20160531/

Latest published version:
http://www.w3.org/TR/webauthn/

Editor's Draft:
http://w3c.github.io/webauthn/

Editors:
Vijay Bharadwaj (Microsoft)
Hubert Le Van Gong (PayPal)
Dirk Balfanz (Google)
Alexei Czeskis (Google)

SE
DI

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

TH
FF

March 2006

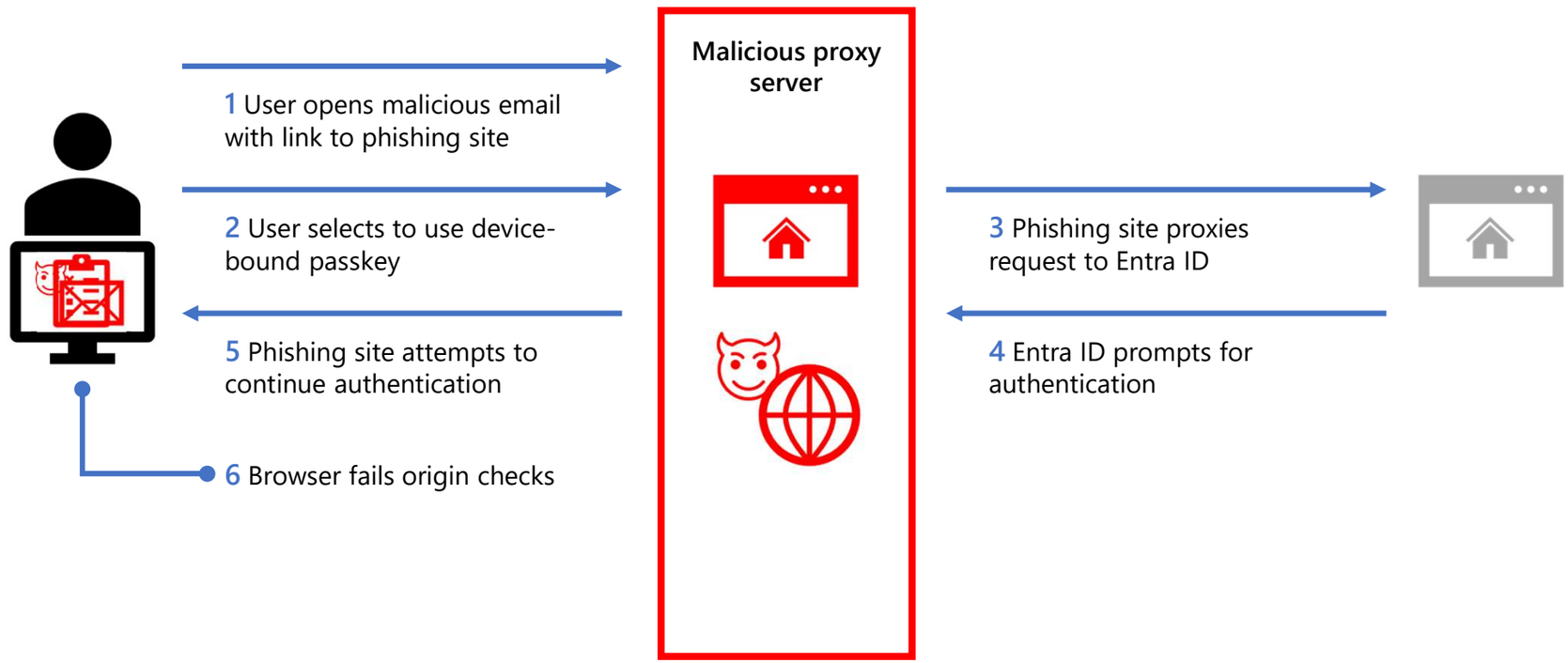
WebAuthn

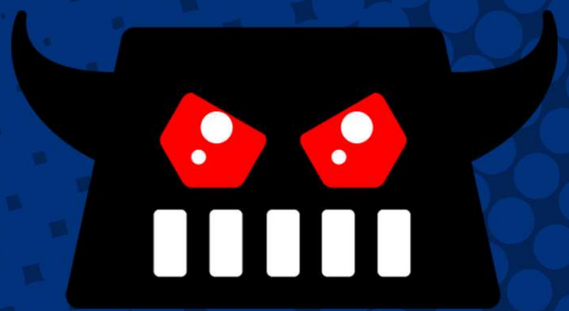
Hybrid Identity Protection

Entra ID Authentication Strengths

Authentication Method	Authentication Model
Device-bound passkey	**Public key**
Windows Hello for Business	**Public key**
Certificate-based authentication (multi-factor)	**Public key**
Microsoft Authenticator Phone Sign-in	**Out-of-band Public Key**
Password + MS Authenticator Push Notification	**Shared secret**
Password + OTP	**Shared secret**
Temporary Access Pass (TAP)	**Shared secret**
Password	**Shared secret**

Modern Phishing Attack - Passkey





Evilginx Demonstration

Hybrid Identity Protection