Webinar

Look Ma, No Password!

Multi-Factor Authentication and Going Passwordless

Thursday, March 30
2pm ET/ 11am PT

NATIONAL CYBERSECURITY ALLIANCE

yubico
Webinar

Please note...

- This webinar is being recorded
  - The recording will be uploaded to staysafeonline.org and Youtube

- Please use the Q&A chat box to ask questions at any time
Today's Speakers

Role
Lisa Plaggemier
Executive Director
National Cybersecurity Alliance

Role
Abby Guha
VP, Product Marketing
Yubico
We empower a more secure, interconnected world.

Our alliance stands for the safe and secure use of all technology.

We encourage everyone to do their part to prevent digital wrongdoing of any kind.

We build strong partnerships, educate and inspire all to take action to protect ourselves, our families, organizations and nations.

Only together can we realize a more secure, interconnected world.
Opportunity

Motivation

Capability

Behavior
“Facts don’t change people’s behavior. Emotion changes people’s behavior.”

*Seth Godin*
Feelings
Poll Question

Q. Staying secure online is under my control.

a. Strongly Disagree
b. Somewhat Disagree
c. Neither Agree nor Disagree
d. Somewhat Agree
e. Strongly Agree
Feelings

Q: How do you feel about cyber security?

Statement:

“Staying secure online is under my control.”
Behaviors
Passwords
Poll Question

Q. What is the typical length of your passwords?

a. Under 6 character
b. 7-8 characters
c. 9-11 characters
d. Over 12 characters
Password Length

- Under 6: 2%
- 7-8: 36%
- 9-11: 46%
- Over 12: 16%
Q. How often do you use unique passwords for your important online accounts (e.g., email, social media)?

a. Never
b. Sometimes
c. Half of the time
d. Most of the time
e. All the time
Q. How often do you use different passwords for your important online accounts (e.g., email, social media)?

a. Never 3%

b. Sometimes 13%

c. Half of the time 20%

d. Most of the time 31%

e. All the time 33%
Q. What is your preferred method of remembering multiple passwords?

a. I write them down in a notebook 37%
b. I write them down in a document on my computer 9%
c. I store them in my phone 13%
d. I store them in my email 6%
e. I just remember them (without writing them down) 22%
f. I save passwords in the browser 6%
g. I use a password manager application 7%
Multi-Factor Authentication
Use of Multi-Factor Authentication (MFA)

43% of the participants had never heard of MFA

Out of the 57% of the participants who had heard about it:

- 79% applied it at least once
- 94% of them reporting that they were still using MFA
Security Behavior

- I started using MFA: 40%
- I'm better at recognizing phishing messages: 58%
- I started saving passwords using a password manager: 35%
- I started saving passwords to a web browser: 31%
- I started using strong and separate passwords: 45%
- I started regularly installing updates: 40%
- I back up my data: 34%
- I did not change any of my online security behaviors: 8%
Peace of Mind
The need for phishing-resistant MFA
82% of breaches caused by stolen credentials

Source: 2022 Verizon Data Breach Investigations Report
Phishing, a growing cyber threat

/ˈfiSHiNG/
The fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Phishing poses the biggest cyber threat
It works!...so very lucrative for malicious actors

<table>
<thead>
<tr>
<th>Cyber crime reported most often</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing/Vishing/Pharming</td>
<td>323.972</td>
</tr>
<tr>
<td>Non-payment/Non-delivery</td>
<td>82.478</td>
</tr>
<tr>
<td>Personal data breach</td>
<td>51.829</td>
</tr>
<tr>
<td>Identity theft</td>
<td>51.629</td>
</tr>
<tr>
<td>Extortion</td>
<td>39.360</td>
</tr>
<tr>
<td>Confidence fraud/Romance</td>
<td>24.299</td>
</tr>
</tbody>
</table>

Source: Statista 2021
So, passwords aren’t great because they’re easy targets for phishing…

but what’s better?
Multi-factor authentication (MFA)

What you know

What you have

Who you are
Not all MFA created equal
Legacy MFA is phishable and easily bypassed by hackers
Cyberattacks Are Bypassing Multi-Factor Authentication

Cyber attackers are learning how to bypass MFA and data centers need to start looking at more advanced security measures. Until then, compensating controls need to be put in place to protect against breaches.

Cybercriminals launching more MFA bypass attacks

New research from Okta shows that cybercrime groups have stepped up their attacks on multifactor authentication systems in an effort to thwart account security measures.
How fake login page defeats legacy MFA

1. Victim
   - Clicks on a link or email

2. Fake login page
   - Enters credentials (UN/PW)

3. Attacker
   - Authenticated on fake site

4. Client web portal
   - Access granted

5. Out of band
   - SMS text
   - Time-based one-time password
   - Mobile push

6. Login successful on fake site

7. Attacker successfully logs into real site
Today attackers don’t hack in, they log in
So what does stop phishing?

True phishing-resistant MFA: Smart Card or FIDO-based authentication
Phishing resistance is the ability of the authentication protocol to detect and prevent disclosure of authentication secrets and valid authenticator outputs to an imposter relying party without reliance on the vigilance of the subscriber.

NIST 800-63B-4 December 16, 2022 (Draft)

Only FIDO2 and Smart Card/PIV (PKI) are phishing-resistant
Portable hardware security keys
Stop phishing in its tracks. Zero account takeovers.

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security key</td>
<td>0%</td>
</tr>
<tr>
<td>On device prompt</td>
<td>10%</td>
</tr>
<tr>
<td>(OTP push app)</td>
<td></td>
</tr>
<tr>
<td>Secondary email</td>
<td>21%</td>
</tr>
<tr>
<td>SMS code</td>
<td>24%</td>
</tr>
<tr>
<td>Phone number</td>
<td>50%</td>
</tr>
</tbody>
</table>
How modern MFA with FIDO stops phishing

1. Victim
2. Fake login page
3. Attacker
4. Client web portal
5. User action not invoked.
6. FIDO credential for real site not phished
7. Unsuccessful login by attacker
Security Keys for Apple ID

Security keys secure iCloud accounts and Apple devices

“Security Keys strengthens Apple’s two-factor authentication by requiring a hardware security key as one of the two factors. This takes our two-factor authentication even further, preventing even an advanced attacker from obtaining a user’s second factor in a phishing scam.”

Apple, January 2023
Modern strong authentication best practices

Consider a portable FIDO/Smart Card-based hardware security key for phishing-resistant MFA
The move to passwordless
The hidden time and cost of passwords

The average user struggles to manage passwords for a dozen or more accounts

- **21 hours**: per person, each year, spent on password resets
- **20-50%**: of helpdesk calls are for password resets
- **$45**: the average estimated cost of a password reset
- **#1**: support cost is password resets
Bridge to passwordless

...and support zero trust initiatives

Phishable to Phishing Resistant

- Password
- SMS Mobile Push OTP
- Smart Card FIDO U2F
- Smart Card FIDO2 WebAuthN

Secure today, future proof for tomorrow
What’s the passwordless user experience?
Frictionless, secure account logins lead to greater productivity

Enter PIN
No password

Touch or tap the security key
Fast login / logout, e.g. shared workstations
Phishing-resistant MFA with the YubiKey
Strong security, passwordless-ready, fast and easy user experience
Summary
Look for an MFA solution that delivers strong protection across your legacy and modern applications and services.
Think past privileged users in an organization…
Remember! When a breach occurs everyone suddenly becomes a privileged user!

- **Privileged access**: Secure privileged account users
- **Mobile restricted**: Secure call centers for mobile restricted users
- **Shared workstation**: Protect shared workstation users
- **Remote workforce**: Enable remote workforce
- **Office workers**: Improve UX and security for office workers
- **3rd party access**: Protect corporate system access by 3rd parties
- **End customers**: Safeguard Yubico customers and end customer
Stay safe online.

Questions?

Website
StaySafeOnline.org

Twitter
@staysafeonline

Facebook
/staysafeonline

LinkedIn
national-cybersecurity-alliance

Email
info@staysafeonline.org