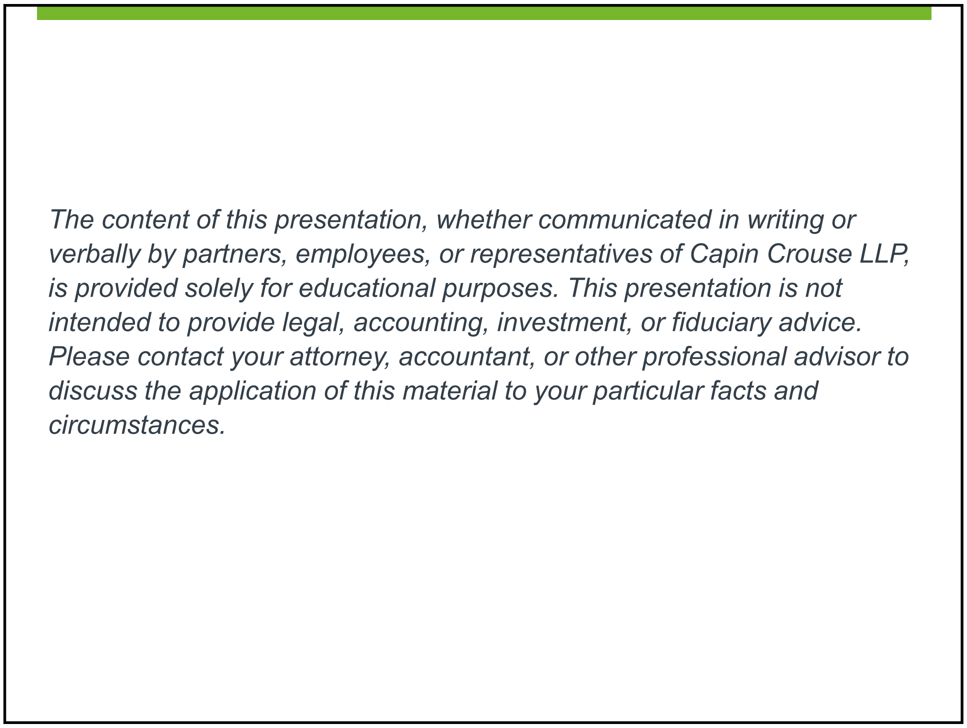
Password Management and Authentication Security

Allison Davis Ward, CISSP, CISA, CISM
Partner, CapinTech
12.1.21



The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

Polling Question 1

Do you want CPE?

Discussion for Today

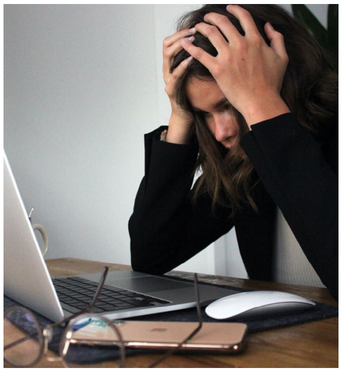
- The state of passwords and authentication
- What does guidance say?
- Baseline best practices
- Trends and newer protections

The State of Passwords and Authentication

CAPINTECH

How We Jeopardize Our Authentication Security

- Common ways we jeopardize our security
  - Use weak passwords
  - Write passwords down
  - Reuse passwords, including for business and personal use
  - Share passwords
  - Never change our passwords
- But why do we do this?



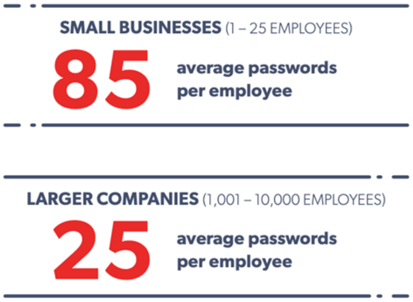
THE 3RD ANNUAL GLOBAL PASSWORD SECURITY REPORT

Emerging trends in access and authentication
in businesses worldwide

LastPass
by LogMeIn

The Password Struggle is Real

- … and tougher for small businesses
- Average passwords per user
  - U.S. – 75
  - Small business – 85
  - Larger companies – 25
  - Not-for-profit – 57

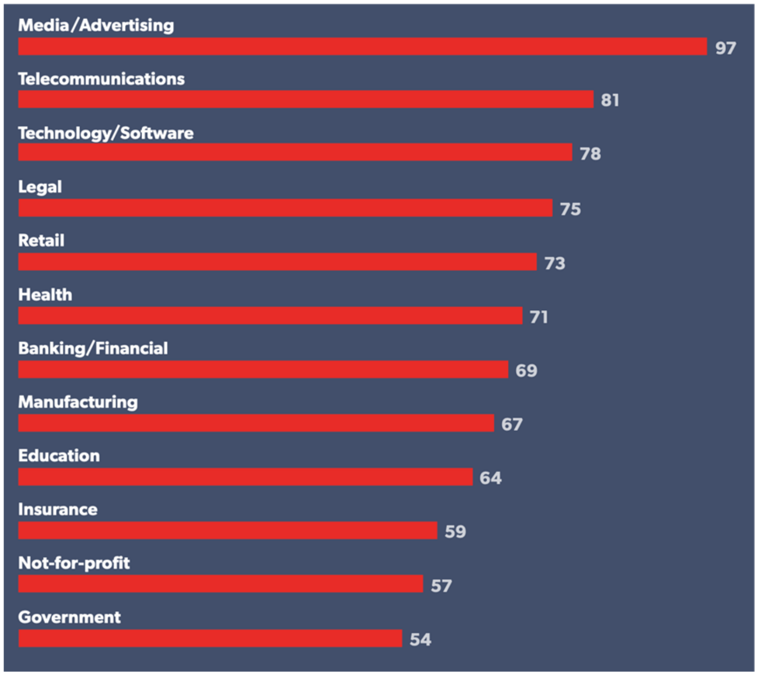


SMALL BUSINESSES (1 – 25 EMPLOYEES)

85 average passwords per employee

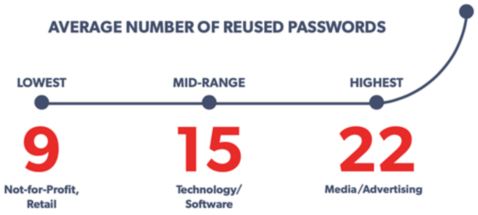
LARGER COMPANIES (1,001 – 10,000 EMPLOYEES)

25 average passwords per employee



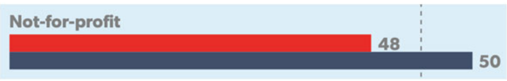
The Password Struggle is Real

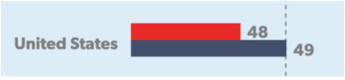
- High rates of password reuse
  - U.S. – 13
  - Small business – 10-14
  - Larger companies – 4
  - Not-for-profit – 9

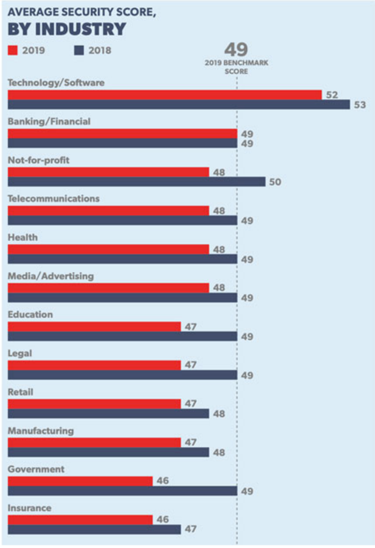


The Password Struggle is Real

- Larger firms improve more year to year
- U.S. security score changed very little but not-for-profit declined slightly





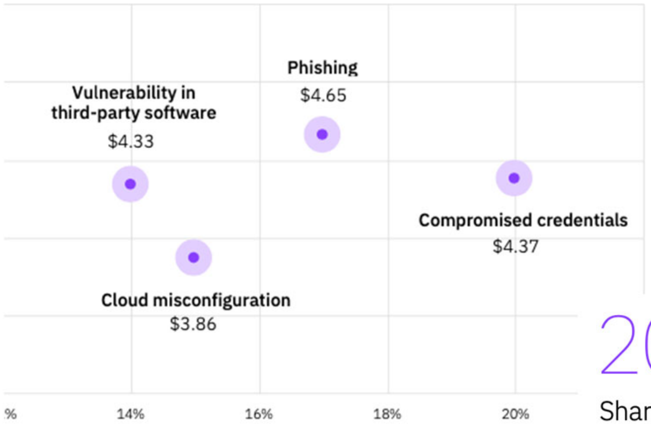


IBM Security

Cost of a Data Breach Report 2021

IBM

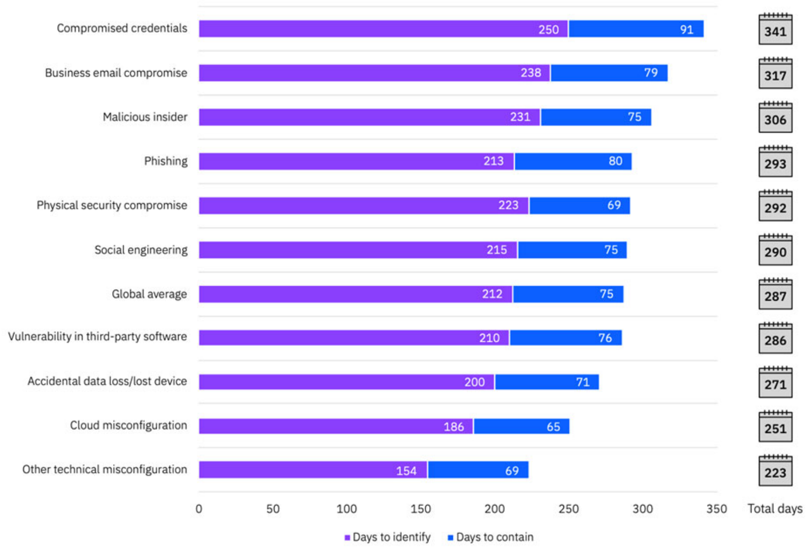
Cost of Top Initial Attack Vectors



20%

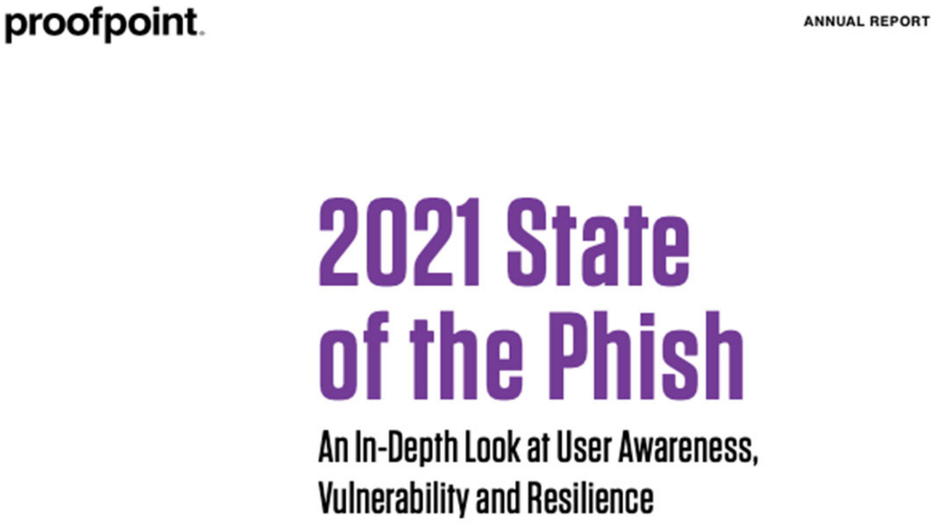
Share of breaches initially caused by compromised credentials

Time to Identify and Contain Breach



Polling Question 2

What is your biggest challenge when it comes to authentication?



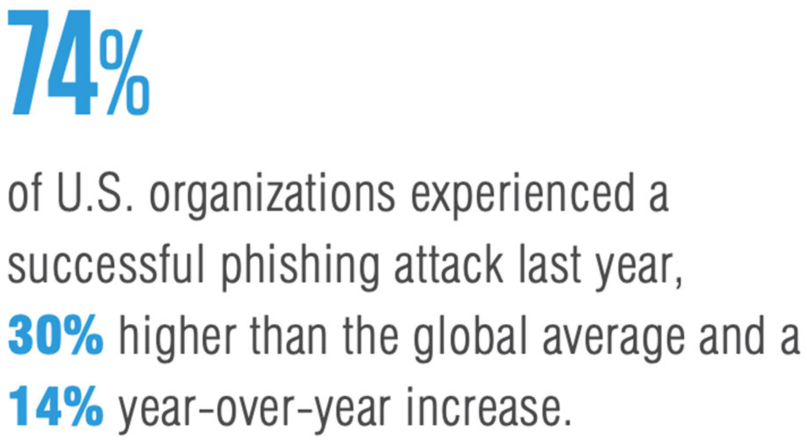
proofpoint.

ANNUAL REPORT

2021 State of the Phish

An In-Depth Look at User Awareness, Vulnerability and Resilience

Phishing Is a Constant Battle

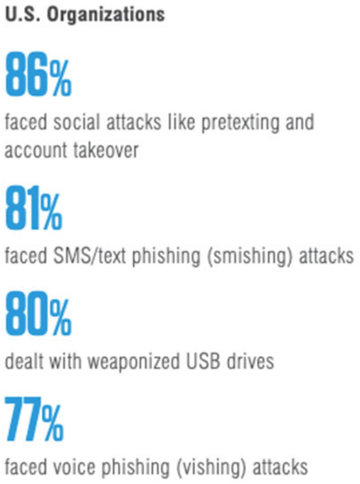


74%

of U.S. organizations experienced a successful phishing attack last year, **30%** higher than the global average and a **14%** year-over-year increase.

As Are Other Methods of Attack

- Social media attacks
- Smishing (SMS phishing)
- Vishing (voice phishing)
- Malicious USB drops



U.S. Organizations

86%

faced social attacks like pretexting and account takeover

81%

faced SMS/text phishing (smishing) attacks

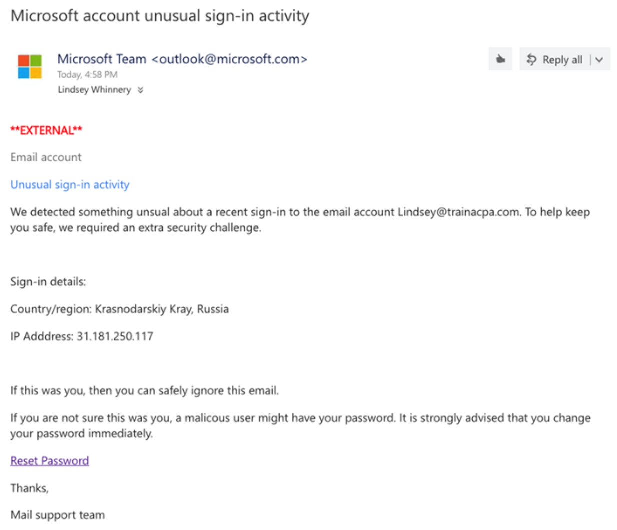
80%

dealt with weaponized USB drives

77%

faced voice phishing (vishing) attacks

Example: Unusual Activity



Microsoft account unusual sign-in activity

Microsoft Team <outlook@microsoft.com>
Today, 4:58 PM
Lindsey Whinnery

EXTERNAL

Email account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the email account Lindsey@trainacpa.com. To help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: Krasnodarskiy Kray, Russia

IP Adddress: 31.181.250.117

If this was you, then you can safely ignore this email.

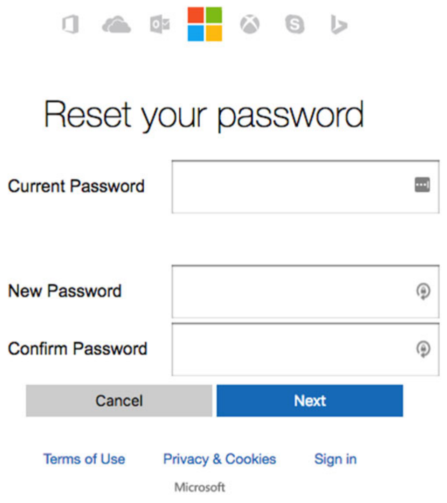
If you are not sure this was you, a malicous user might have your password. It is strongly advised that you change your password immediately.

Reset Password

Thanks,

Mail support team

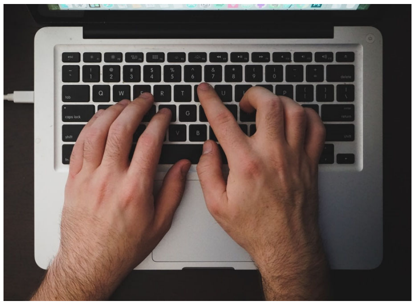
… Leads to Password Reset



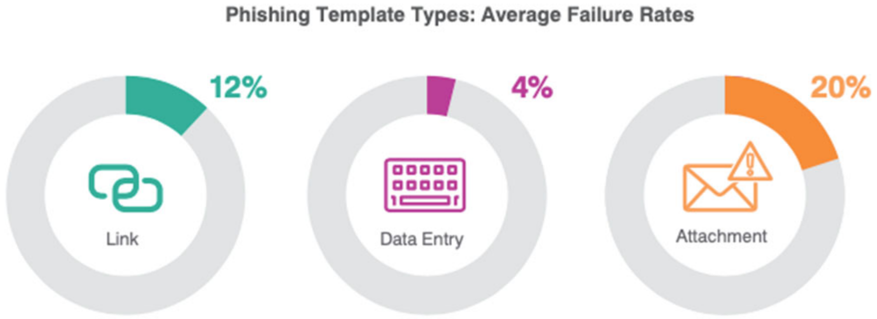
Reset your password

… Or Installation of Keylogger Malware

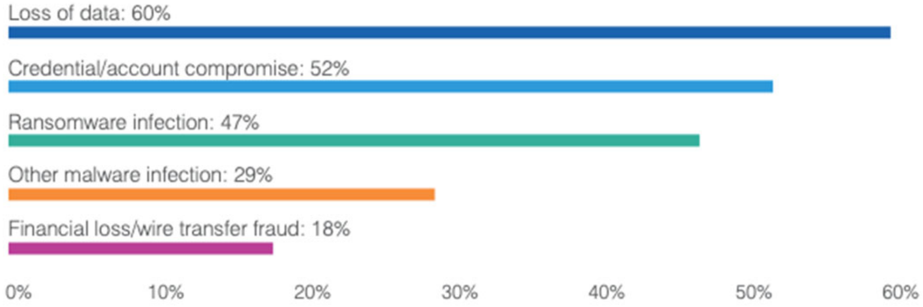
- Captures keystrokes
  - Account information
  - User IDs and passwords
- Huge risk to cloud services
  - Financial systems
  - Email
  - Remote access



Overall Average Failure Rate: 11%



Impacts of Successful Phishing Attacks



Most-Used Phishing Themes

- Office 365 (systems we use)
  - New Microsoft Teams request
  - Office 365 password expiration notice
  - Deactivation of OneDrive account
- Current events (COVID-19 updates)
- Tried and true (UPS and Starbucks)

Trickiest Phishing Themes

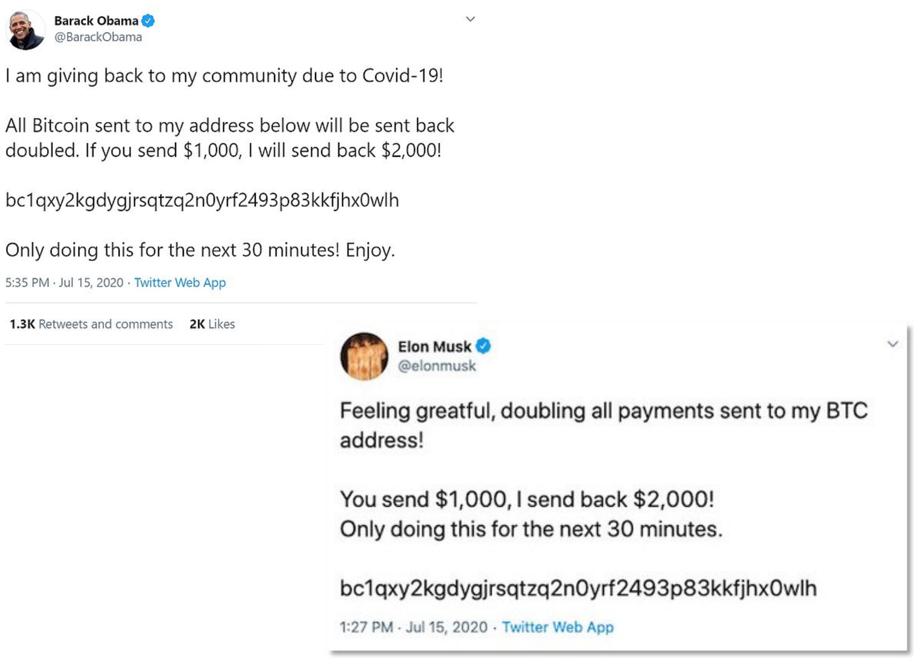
- Free month of Netflix streaming for employees
- Vacation contract rental
- Starbucks pumpkin spice season
- Olympics advanced ticket sales
- Overdue invoice and promissory note
- Spotify password update prompt
- Dress code violation and notice of moving violation

Magellan HEALTH℠ April 2020

- Malware installed internally to capture employee logins
- Launched a phishing attack that allowed them to gain access to a corporate server
- Ransomware installed and data exfiltrated
  - 365,000 patient records determined to be breached initially
  - HHS OCR breach portal now shows 1+ million records impacted

July 2020

- Vishing attack allowed hacker to gain access to internal systems
- Hacker targeted and stole additional credentials
  - Able to access Twitter’s account support tools
  - Accessed 130 Twitter accounts of high-profile people
  - Posted requests for bitcoin transfers and stole $121k
- Twitter promised to further secure systems and roll out additional training



Barack Obama
@BarackObama

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

5:35 PM · Jul 15, 2020 · Twitter Web App

1.3K Retweets and comments 2K Likes

Elon Musk
@elonmusk

Feeling greatful, doubling all payments sent to my BTC address!

You send $1,000, I send back $2,000!
Only doing this for the next 30 minutes.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

1:27 PM · Jul 15, 2020 · Twitter Web App

Colonial Pipeline Company May 2021

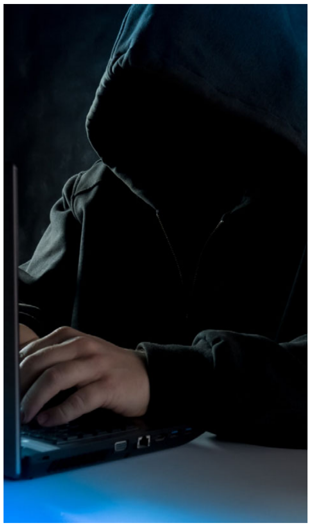
- VPN account used to gain entry to the network
  - Stale account no longer in use
  - Still active with network access
  - No multi-factor authentication
- Password to this account found to be on dark web
  - Could be an indicator of reuse of password

What Does Guidance Say?

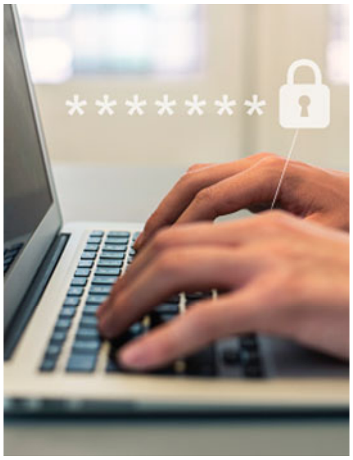
CAPINTECH

Traditional Controls May Not Be Effective

- Controls circumvented over time
  - Remembering passwords is hard, especially with frequent changes
  - Password-cracking software is more sophisticated
  - Social engineering and keyloggers are effective
  - Millions of passwords in circulation due to breaches



Traditional Controls May Not Be Effective



- Can encourage bad practices
  - Creation of predictable passwords
  - Encourage us to store in unsecured manner
- Stolen credentials are often used as soon as they are compromised

NIST Authentication and Lifecycle Management

- Focus shifting to layered security
  - Comparing passwords to “blacklists”
  - Scaling back on forced composition rules or required arbitrary changes
  - Limiting invalid password attempts
  - Enabling multi-factor authentication (MFA)

NIST Authentication and Lifecycle Management

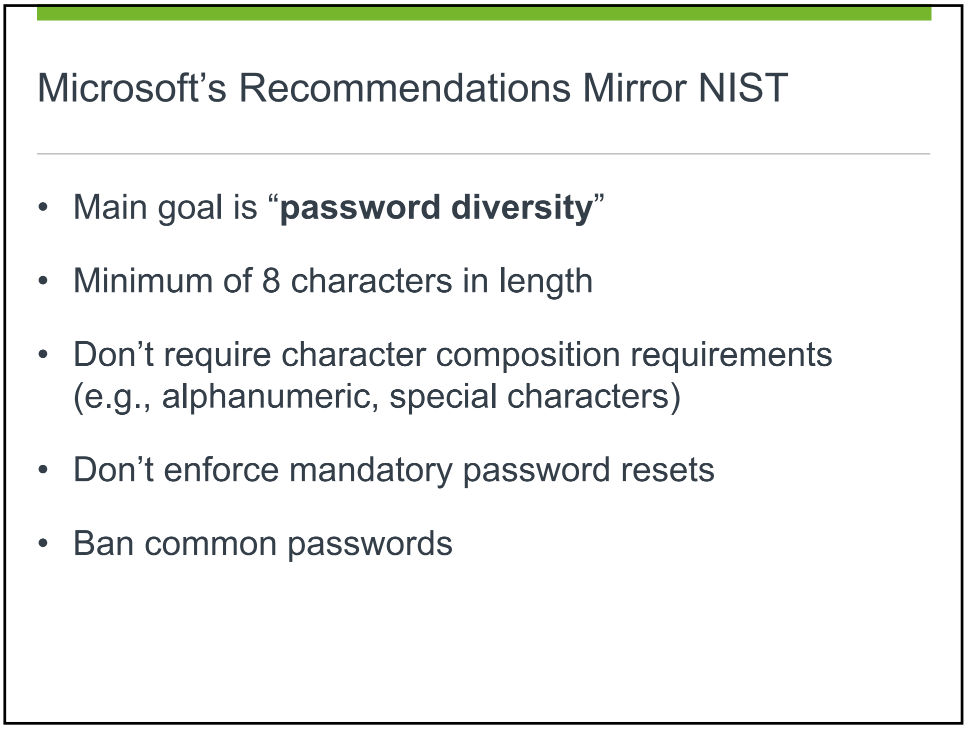
- Blacklists will reject certain passwords and continue to prevent simple passwords
  - Used in previous compromises
  - Based off dictionary words
  - Repeating or sequential characters
  - Based off username, system name, etc.

NIST Authentication and Lifecycle Management

- Length of passwords still important
- Many industry experts still consider complexity and expiration important for high-risk systems
- Changes to vendor systems likely will be slow
- **Should not forgo complexity and expiration if you do not have other mitigating layers**

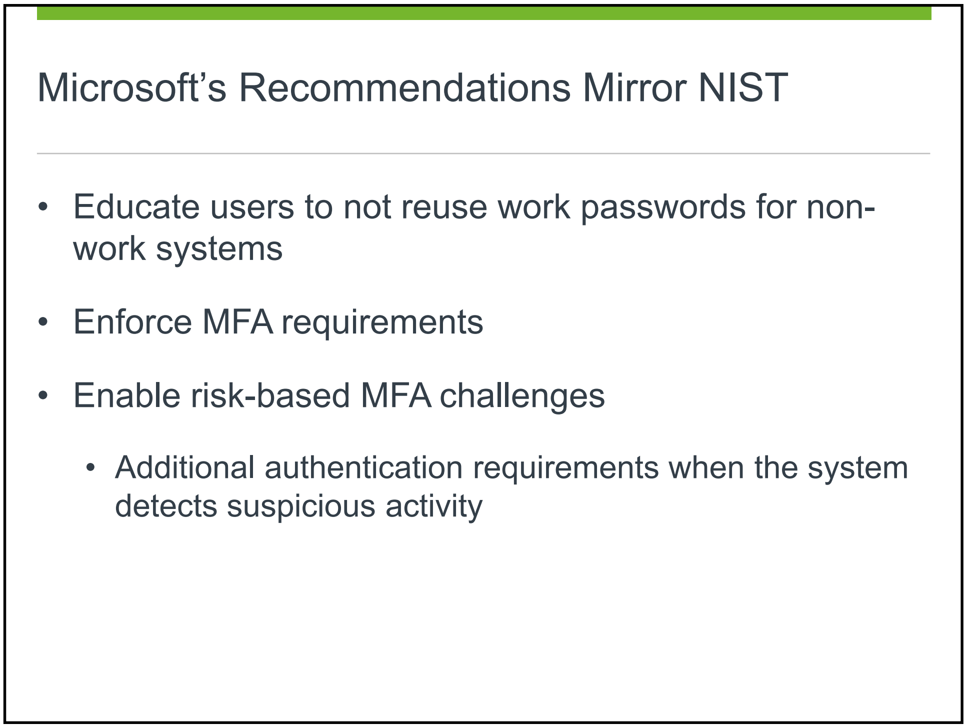
Polling Question 3

What was the biggest change you made as a result of the updated guidance from NIST?



Microsoft’s Recommendations Mirror NIST

- Main goal is “**password diversity**”
- Minimum of 8 characters in length
- Don’t require character composition requirements (e.g., alphanumeric, special characters)
- Don’t enforce mandatory password resets
- Ban common passwords



Microsoft’s Recommendations Mirror NIST

- Educate users to not reuse work passwords for non-work systems
- Enforce MFA requirements
- Enable risk-based MFA challenges
  - Additional authentication requirements when the system detects suspicious activity

Baseline Best Practices

CAPINTECH

Best Practices: Four Categories

- Policies and standards
- Training and awareness
- Control enforcement
- Monitoring
  - Don’t set and forget!

Policies and Standards

- Define your stance related to authentication
  - Requirements for creation and maintenance
  - Proper storage and use of tools
  - How to report issues
- Require formal acceptance of standards upon hire and periodically thereafter

Training and Awareness

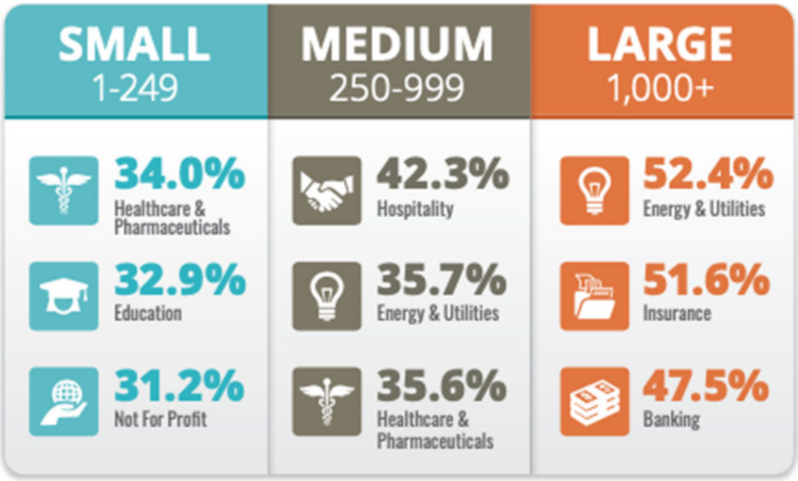
- Communicate standards — don’t rely on policy alone!
- Discuss current threats and challenges
  - Ensure staff understand the ‘why’ for controls
- All employees should participate
  - Culture comes from top
  - Management should not be exempt

KnowBe4

PHISHING BY INDUSTRY 2021

BENCHMARKING REPORT

Phase 1: Baseline Phishing Test Results



SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
34.0% Healthcare & Pharmaceuticals	42.3% Hospitality	52.4% Energy & Utilities
32.9% Education	35.7% Energy & Utilities	51.6% Insurance
31.2% Not For Profit	35.6% Healthcare & Pharmaceuticals	47.5% Banking

Phases 1, 2, and 3: See the Improvement?

Phishing Test Results: Nonprofit Industry

Phase	1 – 249 Employees	250 – 999 Employees	1,000+ Employees
1 (no training)	31.2%	31.5%	40.8%
2 (90 days after training)	19.1%	19.6%	18.0%
3 (1 year after training)	4.3%	4.4%	5.1%

KnowBe4 “Phishing by Industry Benchmarking Report”

Training and Awareness Reminders

- Don’t share or reuse
  - Business ≠ personal
- Keep them off your desk
  - Don’t write down in plaintext
  - Consider password managers
- Encourage creation of non-predictable passwords

How to Identify Phishing

- Inspect for typos
- Check email address and domain name
  - joe@alliedconsulting.com
  - joe@alIiedconsulting.com (capital I vs. lowercase l)
- Click correctly
  - Hover over link
  - Visit website manually

How to Identify Phishing

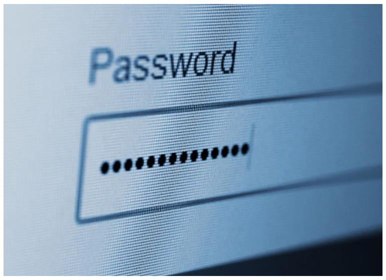
- Does it require you to click link or open attachment?
- Does it feel right? Is the tone off?
- Is it urgent or threatening?
- Is it unfamiliar or unexpected?
- In doubt? Pick up the phone!

Control Enforcement: Administer Your Users Well

- New employee, internal transfer, terminations
- Grant access to support job function
- Vendor/contractor/auditor
- Extended leave
- Board members

Control Enforcement: Password Requirements

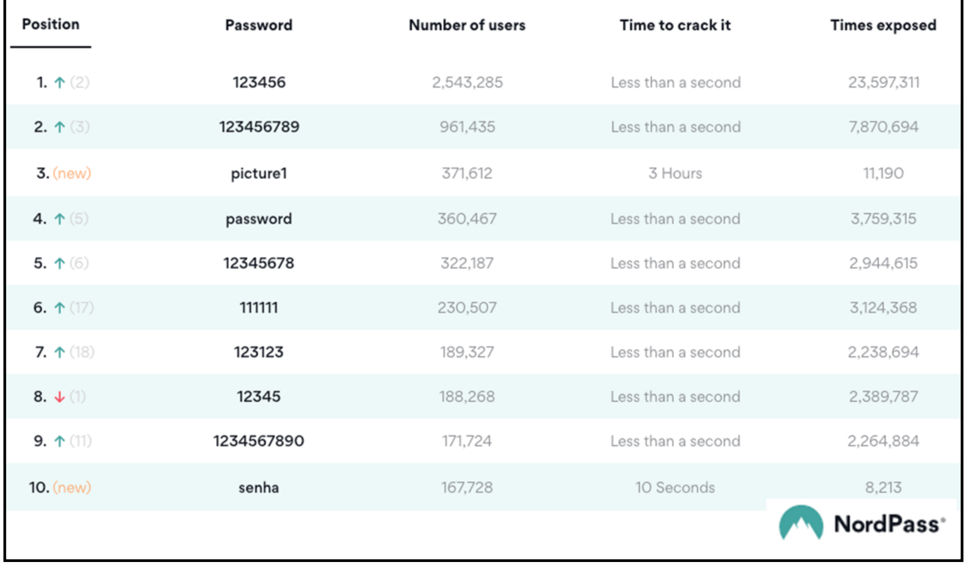
- Do your settings support password diversity?
- Do your settings encourage the creation of non-predictable passwords?
- What controls support this?



Control Enforcement: Password Requirements

- What helps support this in your organization?
  - Numbers, characters, symbols, passphrases
  - Length requirements
  - Use of passphrases
  - Periodic expiration
  - Usage of blacklists and avoiding common passwords
- One size does not fit all

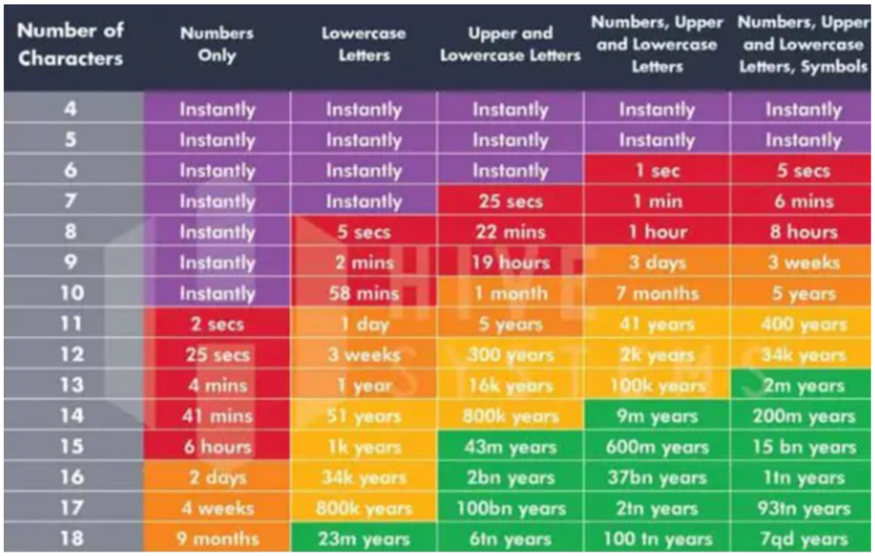
Why We Need to Enforce Certain Settings



Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,543,285	Less than a second	23,597,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (11)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213

NordPass

Why Length (and Complexity) Can Be Important



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Control Enforcement: Other Layers

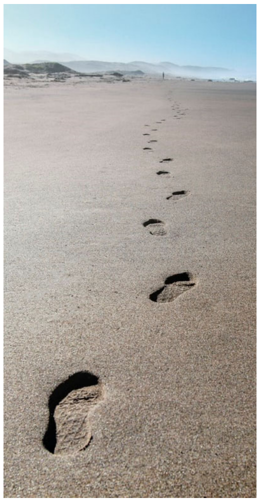
- Prevent saving passwords in browser
- Inactivity timeouts (<15 minutes)
- Account lockout settings
- IP/country restrictions
- Time and day restrictions

Control Enforcement: MFA

- Critical for cloud and high-risk applications
  - Remote access, email, file transfer, data storage
- Something you know + something you have and/or something you are
  - Password (know) + fingerprint (are)
  - Password (know) + authenticator app (have)
  - Facial recognition (are) + text code (have)

Control Enforcement: Audit Logs

- Can’t manage what you can’t measure
- Configure auditing to leave a trail
  - Successful/failed attempts
  - User administration changes
  - Excessive privilege use
  - Denied permission activity
- Configure a log retention

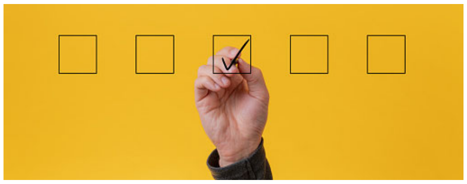


Control Enforcement: Ancillary Endpoints

- Don’t forget about other endpoints
  - Network infrastructure
  - Wireless routers
  - Mobile devices
  - Internet of Things
- Change default passwords and at least annually thereafter

Monitoring

- Periodic review of access to applications
  - Who/what can authenticate and to what extent?
  - Employees, vendors, system accounts
  - Review access rights, including privileged access
  - Question stale accounts



Monitoring

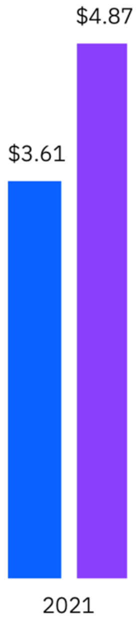
- Annual review of policy standards
- Periodic review of configured settings
  - Do we still feel comfortable with configured settings?
  - Do they still meet industry best practices?
  - Have they become misconfigured?

Monitoring

- Incident response is an IT issue… but every department plays a role
- Effective incident management requires quick identification
- Review suspicious activity
  - Real-time notifications or alerts
  - Scheduled review of lots
- Establish process to respond promptly

Monitoring

- Why is time so important?
  - Lifecycle < 200 days – $3.61M
  - Lifecycle > 200 days – $4.87M
- Preparation pays
- Walk through your department’s role in the organization’s plan



Monitoring: Preparing for Incidents

- What would trigger escalation?
- What looks suspicious?
- Who would we call?
- Application-specific steps?
  - Ex: checking for auto-forwarding rules that were created in a compromised email account

Trends and Newer Protections

CAPINTECH

Polling Question 4

Are you using any of the following tools to help strengthen authentication?

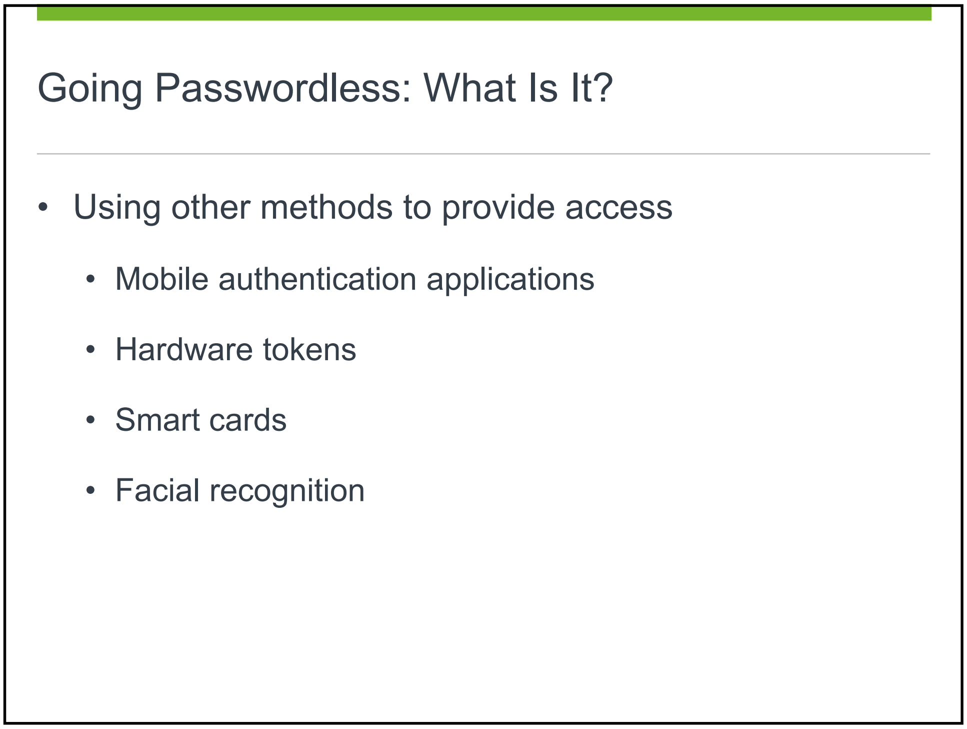
Enterprise Password Management Tools

- Help create strong passwords and store securely
  - Necessary to have strong master password and MFA
- Various controls available based on platform
  - Restrict access to certain countries
  - Prevent login from anonymous browsers (e.g., TOR)
  - Check passwords against breached passwords
  - View “security scores” for registered users

Sigle Sign On (SSO) Solutions

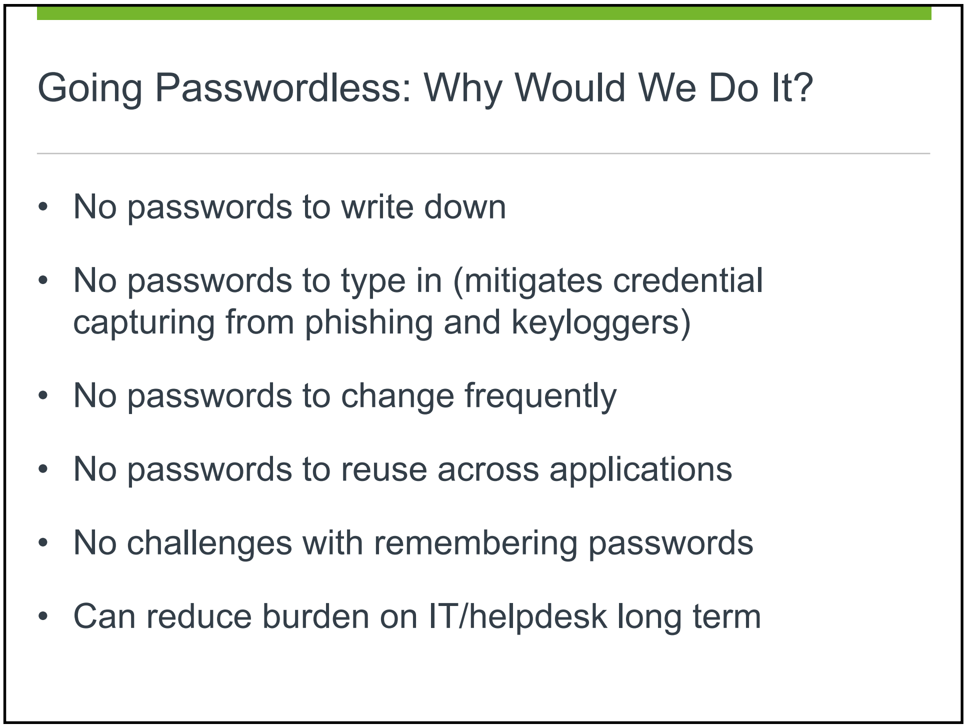
- Enforce more stringent authentication parameters
  - Only one password to remember
  - Couple with strong MFA layer
  - All other logins tied behind master
- Use blacklists and force password reset if breached

DUO okta onelogin



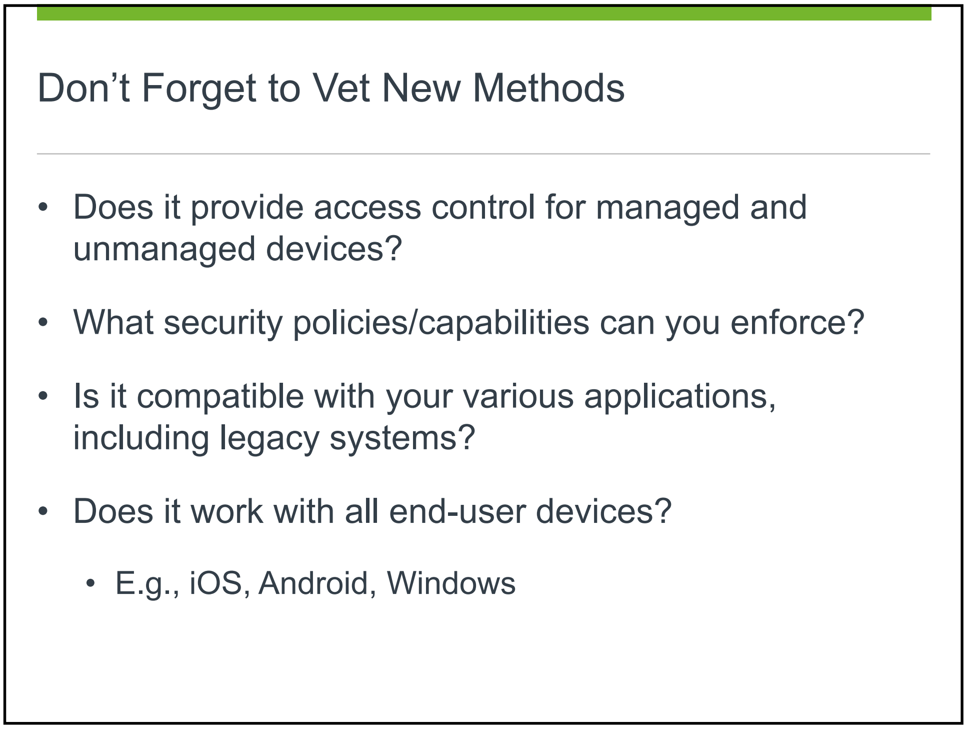
Going Passwordless: What Is It?

- Using other methods to provide access
  - Mobile authentication applications
  - Hardware tokens
  - Smart cards
  - Facial recognition



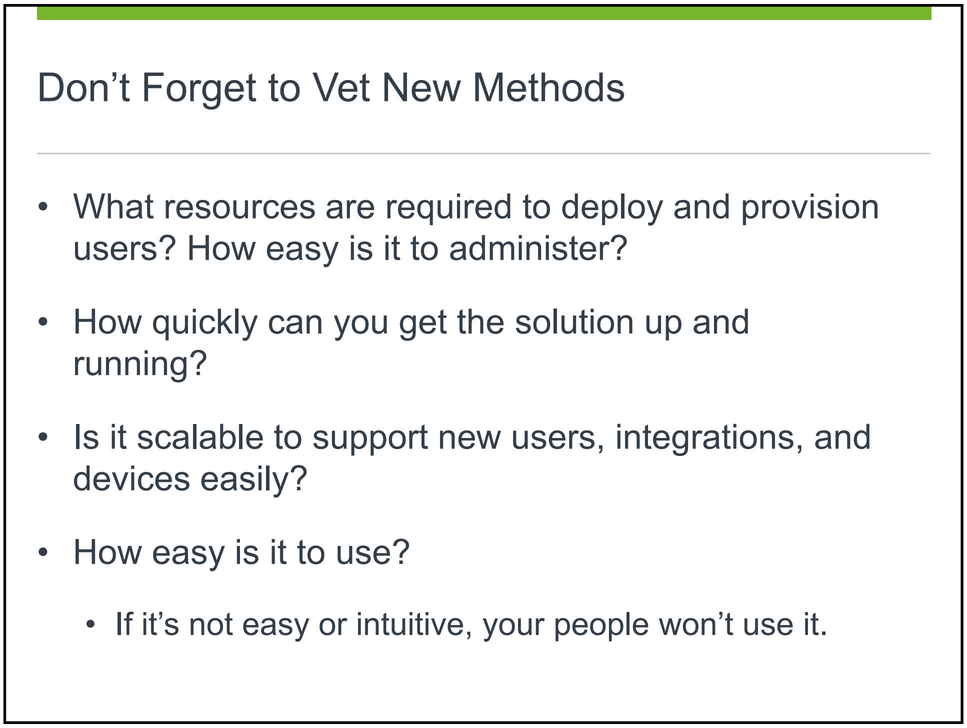
Going Passwordless: Why Would We Do It?

- No passwords to write down
- No passwords to type in (mitigates credential capturing from phishing and keyloggers)
- No passwords to change frequently
- No passwords to reuse across applications
- No challenges with remembering passwords
- Can reduce burden on IT/helpdesk long term



Don’t Forget to Vet New Methods

- Does it provide access control for managed and unmanaged devices?
- What security policies/capabilities can you enforce?
- Is it compatible with your various applications, including legacy systems?
- Does it work with all end-user devices?
  - E.g., iOS, Android, Windows



Don’t Forget to Vet New Methods

- What resources are required to deploy and provision users? How easy is it to administer?
- How quickly can you get the solution up and running?
- Is it scalable to support new users, integrations, and devices easily?
- How easy is it to use?
  - If it’s not easy or intuitive, your people won’t use it.

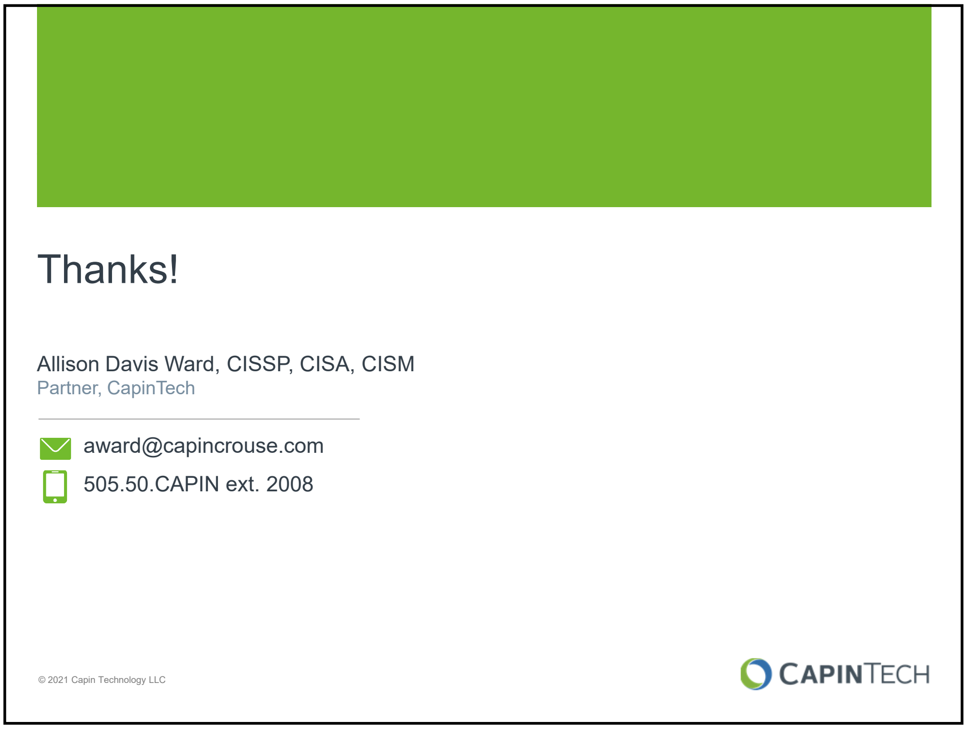
Don’t Forget to Vet New Methods

- Is the provider distributed geographically?
  - You do not want downtime!
- Does it allow audit capabilities and alerting of issues?
- Are the dashboards user-friendly so that IT can be effective in managing?
- Take a holistic approach or you could leave various aspects of your environment vulnerable.

You Could Win a Free CapinTech Cyber Checkup!

- Receive one entry for each 2021 CapinTech Cyber Series webcast you:
  - Attend live, or
  - Watch the recording of within one week of the webcast date
- Winner announced December 13th

CAPINTECH
Cyber Series
Free webcasts exploring the latest cybersecurity issues and risks.



Thanks!

Allison Davis Ward, CISSP, CISA, CISM
Partner, CapinTech

✉ award@capincrouse.com
📱 505.50.CAPIN ext. 2008

CAPINTECH