



Enhancing Password Security and the Power of Multi-Factor Authentication



NPC Safe Computing Webinar Series

January 17th, 2023

Larry Keating, President
Darren Mar, National Sales Manager

Copyright © NPC DataGuard 2023. A division of Compugen Inc.

Thank You!



Presenters



Larry Keating
President

30+ years' experience with information technology, remote communications and data security.



Darren Mar
National Sales Manager

10+ years in SMB technology products and services, with emphasis on financial services small office security.

Agenda

Passwords and Passphrases

Multi-Factor Authentication

Password Policy and Management

Q & A



Passwords and Passphrases

Common Misconceptions

Replacing letters with digits or symbols allows you to use a shorter password:

- Like a "\$" for "5" or a "3" for an "E"



Ordinary words are never OK to use in a password



If it's really strong, you can use a password in different systems



When you are only allowed three attempts, a simpler password is fine



You should never write your passwords down



REALLY?!



Some Password Truths

- The more scrambled, the harder it is for a human to type or remember
 - A computer processes information and makes calculations different than a human
 - What looks scrambled to us, may not be a challenge for the computer
- The more frequently we force password changes, the more likely it is we will start to use weaker, easier to remember passwords
- So, people use simpler, shorter passwords, or reuse them, weakening password security

**We've made passwords easy for computers to guess,
but hard for people to remember (or type)**

NIST Guideline Evolution

- No longer recommending frequent password changes
 - Unless there has been an indicator of compromise or an actual attack
- No longer recommending symbol or character gobbledygook (What the ?%\$#!)
- (To do this, implementation of the full NIST recommendation should be in place)

So now, password length really matters

Passwords and Passphrases

Favour **length** over complexity.

Create a passphrase that is a **memorable** mental image for you.

Try to use one **uncommon** word.



Passwords and Passphrases

How Secure is Your Password?

Take the Password Test

Tip: Try to make your passwords at least 15 characters long

Show password: ☒

Melis3a!



Very Weak

8 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:
59.36 seconds

Review: Oh dear, using that password is like leaving your front door wide open. Your password is very weak because it contains 3 dictionary words and a female name.

Passwords and Passphrases

How Secure is Your Password?

Take the Password Test

Tip: Avoid the use of dictionary words or common names, and avoid using any personal information

Show password: ☒

melissa skate f@ll up



Very Strong

21 characters containing:

Lower case

Upper case

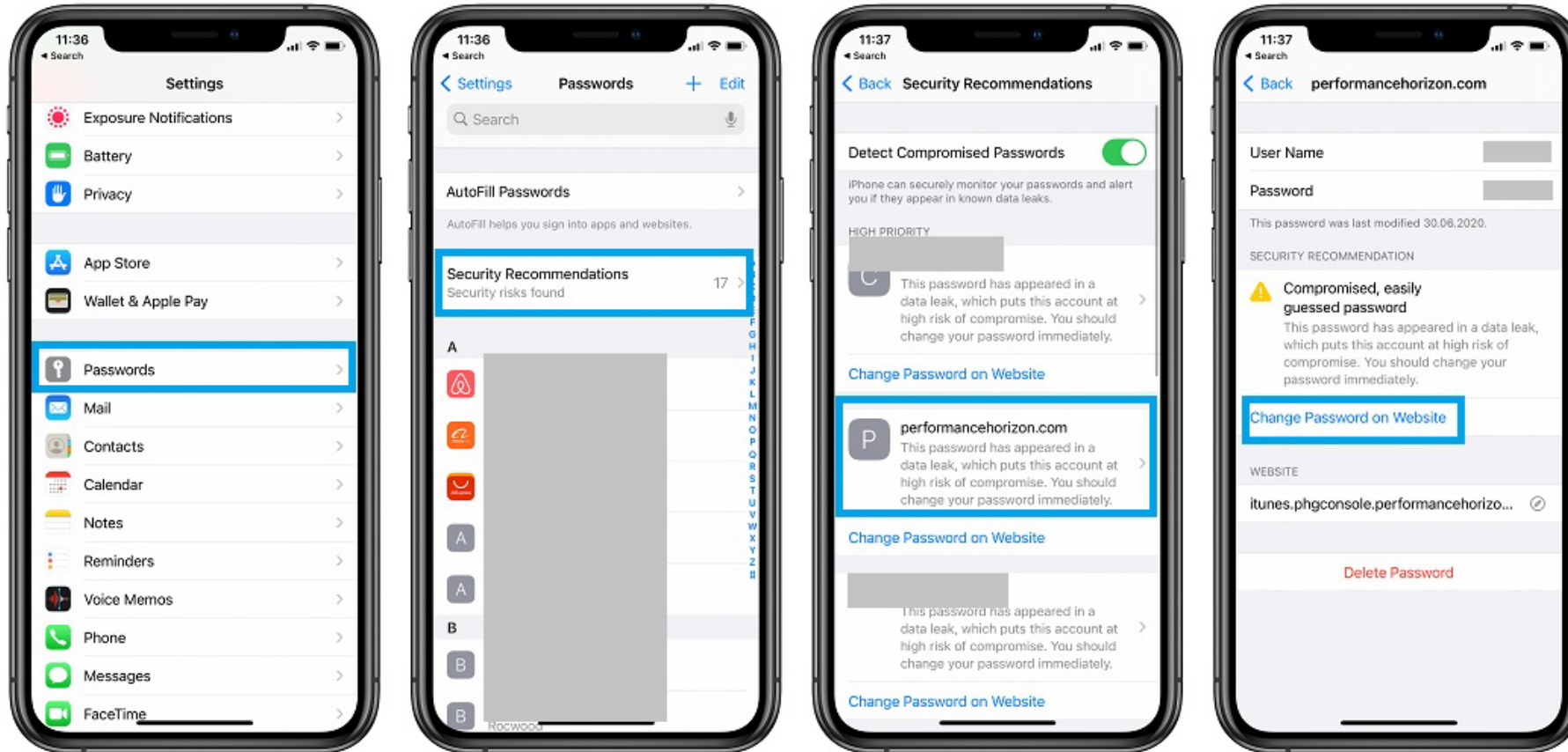
Numbers

Symbols

Time to crack your password:
30 centuries

Review: Fantastic, using that password makes you as secure as Fort Knox.

Passwords Security Recommendations



Passwords and Passphrases Best Practices

- ☐ Use passphrases, favour length over complexity
- ☐ Always use two-factor / multi-factor authentication
- ☐ Never text or email a password with the login name, or what system or service it is used for
- ☐ Never use the same password twice, or in more than one place:
 - Have I Been Pwned <https://haveibeenpwned.com/>
- ☐ Never use easy to guess security confirmation questions, especially if you have published that detail on social media
- ☐ Never confirm a password online through a link you are uncertain of, never give it up over the phone or in a text



Save this **checklist** for later.

Passwords and Passphrases

Best Practices

- ❑ Use fingerprint readers
 - Allows longer passwords and passphrases, without the inconvenience of having to frequently type them
- ❑ Use different passwords strengths for different services:
 - Know when a system allows limited or unlimited password attempts
 - Use a very strong passphrase, in excess of 20 characters, if a site has unlimited attempts
- ❑ Use password management tools provided with business-class computers
- ❑ Unless you are on a secure device and using a security tool like Hello, never embed personal financial info or credentials for important sites in your browser
- ❑ Online password managers that centralize all your passwords should be very carefully researched and considered



Save this **checklist** for later.

Writing Passwords Down

- ☐ If you don't use a Password Manager, writing them down may be required
- ☐ Can enable better password hygiene
- ☐ Most passwords are stolen electronically. If it is not physically written down, ensure it is done in an encrypted form on a secured drive or computer

Follow these practices:

- ☐ Be certain that how you are storing and managing your list is secure
- ☐ Do not (fully) write down the associated usernames or site/services they are for. But know that for most of your logins it is your email address, and that is known
- ☐ Change the written down password slightly, but do not make the change uniform across all your passwords



Save this **checklist** for later.



Multi-Factor Authentication

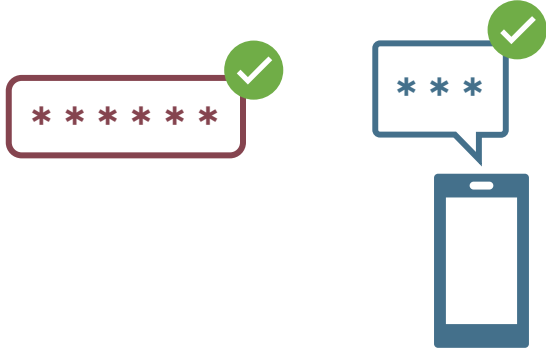
Multi-Factor Authentication

Definition:

A method of allowing access to applications, websites, systems or devices, only after the user presents two or more pieces of authentication evidence.



Multi-Factor Authentication Definitions



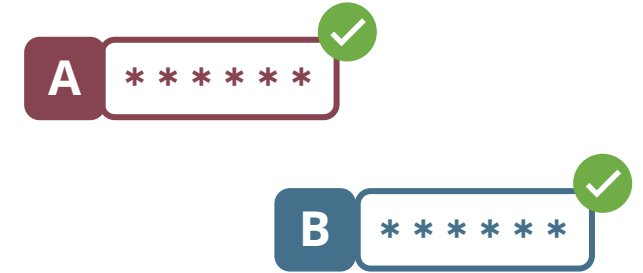
2FA: Two-Factor Authentication

Following the login or password, the user is offered only one additional factor.



MFA: Multi-Factor Authentication

The user has a choice of second factor method or is required to complete two additional factors.



Two-Step Verification or Authentication

Repeating the same authentication process but requiring different variable input.



MFA Benefits

“Organizations that neglected to implement multi-factor authentication, along with virtual private networks (VPN), represented a significant percentage of victims targeted during the pandemic.”

Verizon 2021 Data Breach Investigations Report

- Creates “defense in depth”
- Can be made to work efficiently for the user

MFA Benefits

"Your account is more than 99.9% less likely to be compromised if you use MFA"

Alex Weinert, Group Program Manager for Identity Security and Protection at Microsoft

- Microsoft reports that 20+ million accounts are probed daily in Microsoft ID systems for Credential Stuffing

Forms of Attacks Prevented

Stops “brute force attacks”,
or account compromise
from lost or stolen
passwords/credentials, or
poorly constructed primary
authentication systems:

Phishing

**Man-in-the-Middle
(MITM) Attacks**

Spear Phishing

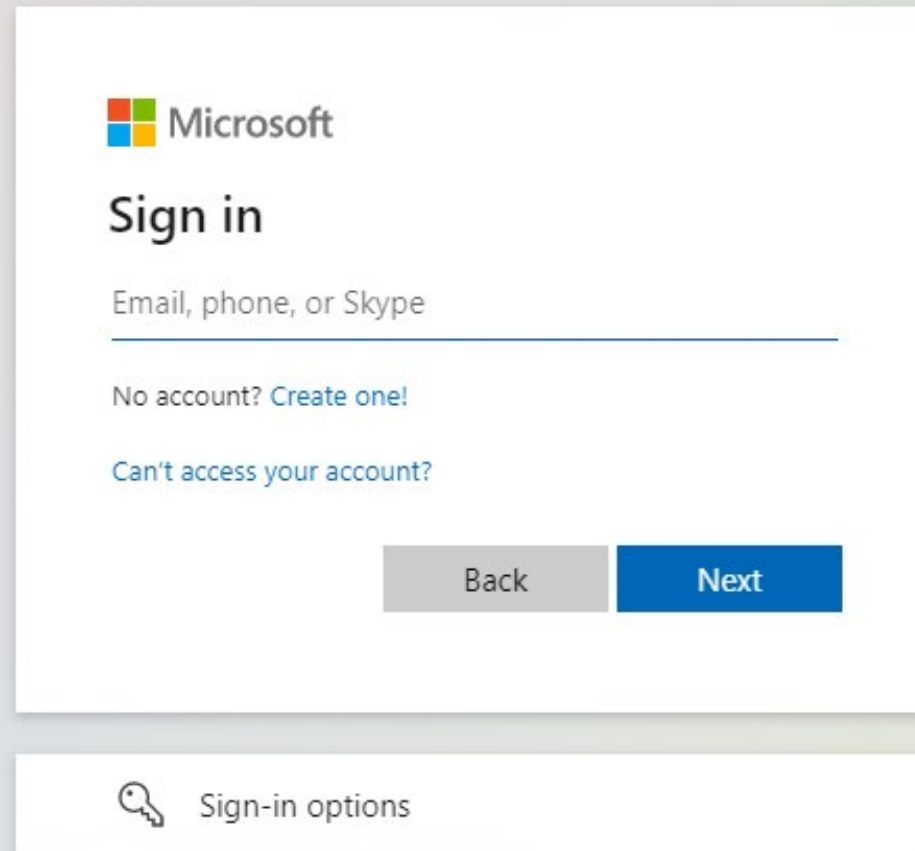
**Credential
Stuffing**

Keyloggers

**Brute-Force
Attacks**

**Reverse
Brute-Force
Attacks**

Microsoft 365 MFA



The image shows a Microsoft sign-in interface. At the top is the Microsoft logo. Below it is the text "Sign in". There is a text input field with the placeholder text "Email, phone, or Skype". Below the input field are two links: "No account? Create one!" and "Can't access your account?". At the bottom of the sign-in box are two buttons: "Back" and "Next". Below the sign-in box is a separate box containing a key icon and the text "Sign-in options".

Microsoft


Sign in

Email, phone, or Skype


No account? [Create one!](#)

[Can't access your account?](#)

Back Next


 Sign-in options


Microsoft 365 MFA

 Microsoft

Ikeating@npcdataguard.com

Verify your identity

 Text +X XXXXXXXX53

 Call +X XXXXXXXX53

[More information](#)


Cancel

Microsoft 365 MFA



lkeating@npcdataguard.com

Enter code

 We texted your phone +X XXXXXXXX53. Please enter the code to sign in.


Code

Having trouble? [Sign in another way](#)

[More information](#)

Verify

Microsoft 365 MFA

 Microsoft

lkeating@npcdataguard.com

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

☐ Don't show this again



Only on **your** secure computer or phone.

Basis of Authentication Methods

Authentication methods are evolving:

- Geo Location - where a user is at that moment:
 - Screening access based on an IP address or, more precisely, the user's geo location can be considered an authentication factor
- Adaptive Authentication, or Risk-based Authentication:
 - Analyzes behaviour or the user's context and increases or decreases authentication requirements accordingly



[Go to Implementation](#)



Passwords Policies and Password Management

Password Policies

- Establish and maintain a Password Policy for your staff
- The policy should contain:
 - Minimum recommendations for length, age, re-use, etc.
 - Do's and don'ts of password hygiene
 - Storing and managing passwords, including termination of employment and ownership of the passwords or access to business services
- Include the policy in your onboarding kit
- Often required for cyber insurance, regulatory requirement, etc.

Password Management

- A Microsoft 365 / SharePoint and Exchange Email subscription includes that ability to enforce minimum password standards and MFA
- Consider a corporate tool like Okta
- Windows Hello, business version, is a secure and convenient password manager for you or your staff
- Some computer and device vendors include a password management tool



Additional Resources

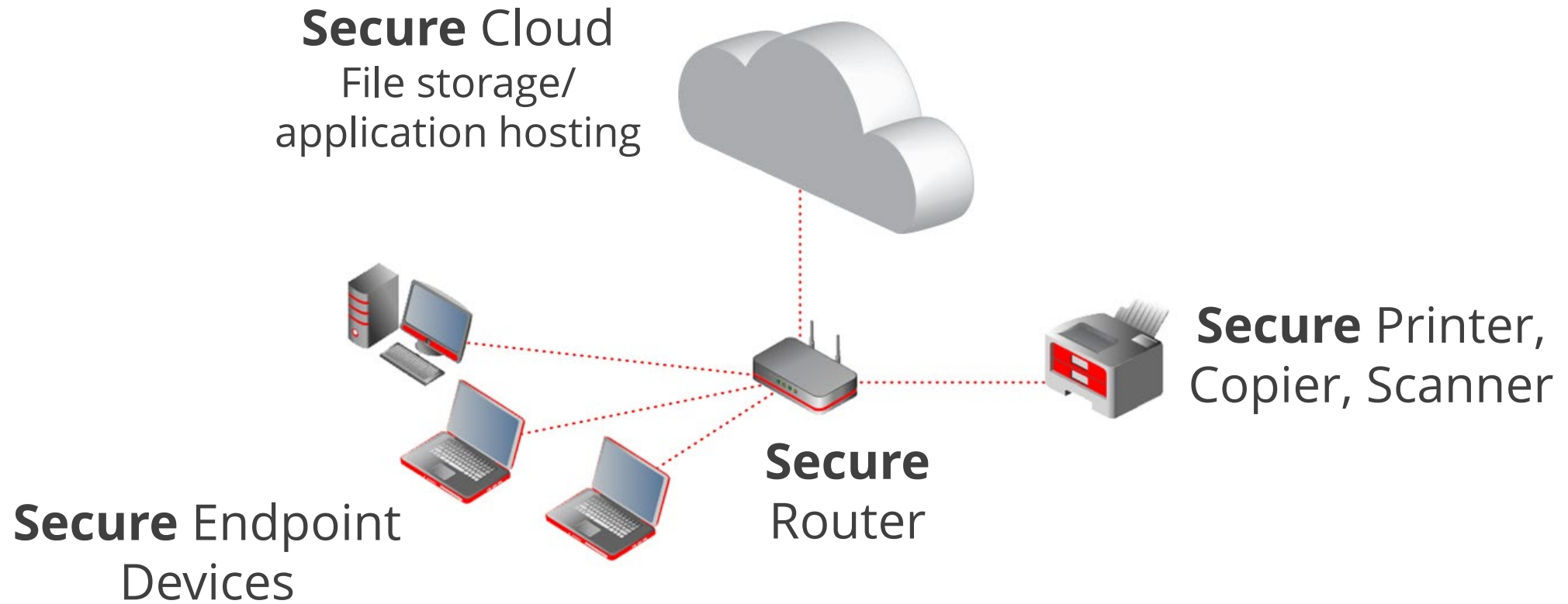
NPC Solutions

Secure managed computers and Microsoft 365 for the professional and SMB office.



- NPC Secure Managed Computers
 - Hardware, encryption, backup, system software, security, technical support, managed and monitored for you
- NPC Managed Microsoft 365
 - SharePoint, Exchange Email, Teams, and a host of productivity tools
- Cyber Assessments and Pen Testing
- Dedicated Account Manager
 - A custom and consultative approach

Office of the Future



NPC Security Alerts



npcdataguard.com/alerts

[Préférez-vous voir ce courriel en Français?](#)

NPC™ Security Alerts



Update: LastPass Reveals Personal Info and Encrypted Passwords Stolen in Recent Breach

[Click here to read the full alert](#)

Note: This NPC Security Alert updates our [alert issued December 12, 2022](#), regarding the LastPass Breach of August 2022.

What is the Issue?

On November 30, LastPass issued a notice that they had suffered a second data breach, following a breach in August. In November they knew that information gathered during the August breach enabled the threat actors to gain access to their systems, but it was unclear exactly what information had been used or what customer data had been compromised.

In an update published on December 22, 2022, LastPass advised they learned from their ongoing investigation that two types of data have been taken: unencrypted basic customer information like company names, end-user names, billing addresses; and encrypted customer “vault data” — client login and password stores.

This presents two problems for LastPass users. First, the unencrypted basic customer information can be employed to help the threat actors break the vaults and to better execute phishing attacks against the users. Second, because the vaults were copied out of the LastPass system, the threat actors now have unlimited time to attempt to break the vaults with the stolen descriptive information about the owner of a vault.

Upcoming NPC Webinars



npcdataguard.com/webinars

January 19th
1:00 PM ET (30 mins)

NPC DataGuard Solutions
Overview

February 14th
1:00 PM ET (60 mins)

Ransomware 2.0: Prevention is
Your Best Option

February 16th
1:00 PM ET (30 mins)

NPC DataGuard Solutions
Overview

NPC Webinars Recordings



npcdataguard.com/webinars

[How to Prepare for the Most Common Cyber Attacks Facing SMBs](#)

[How to Protect Your Business from Email Compromise Attacks](#)

[Implementing and Managing the Secure Hybrid Workplace](#)

[Building an Incident Response Plan for the SMB](#)

+ New Topics Will Be Added in 2023!

Q&A

Larry Keating

lkeating@npcdataguard.com

905-305-6501

Darren Mar

dmar@npcdataguard.com

905-305-6513



Thank You

Please Be Safe & Stay Healthy



NPCTM
Smarter Computing



Multi-Factor Authentication Implementation Considerations

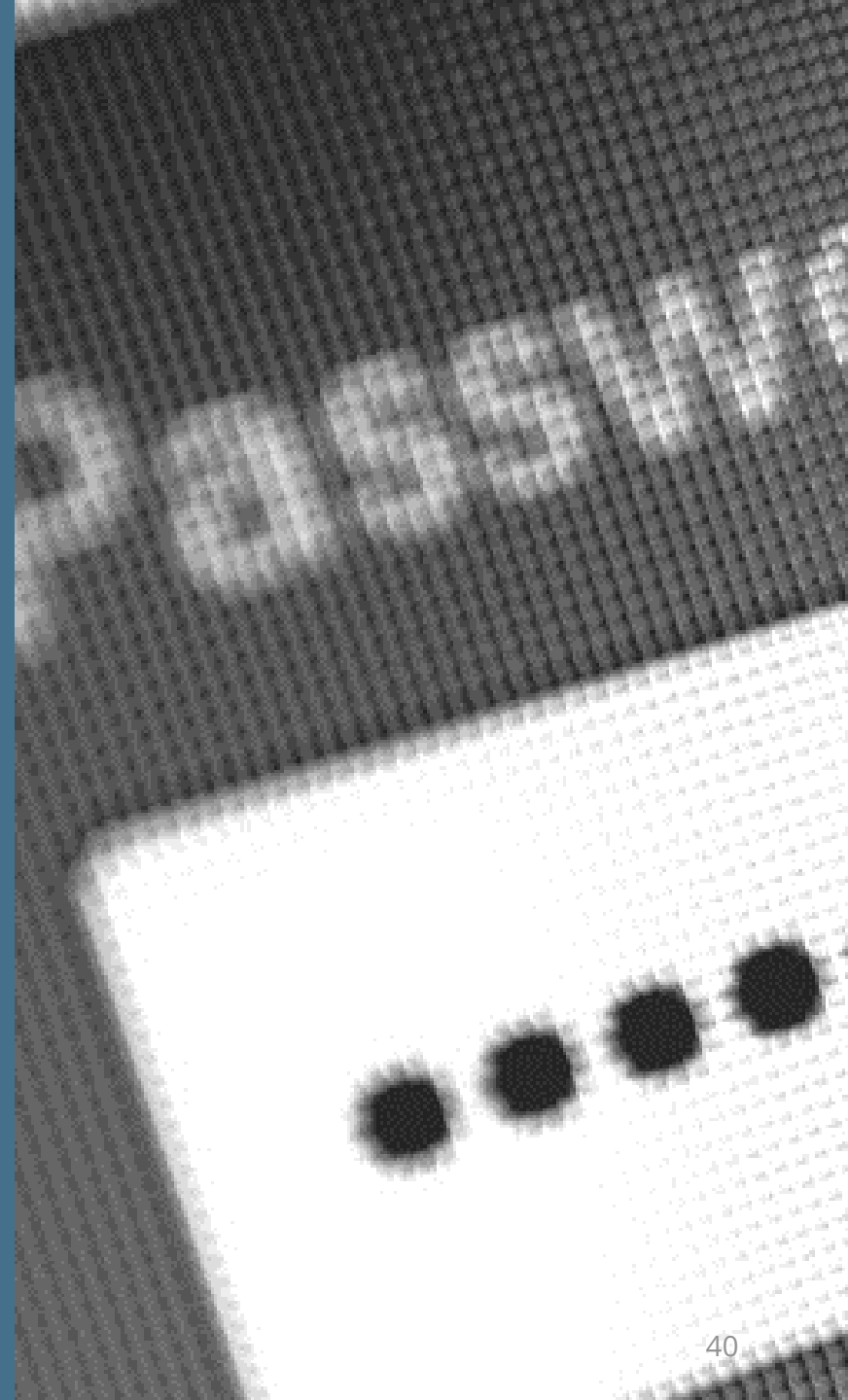
Basis of Authentication Methods

Step 1

What the user **knows**
(1st Authentication) such as:

- Password
- PIN
- Security question

Authentication methods are based on principles that each one is independent of the other.



Basis of Authentication Methods

Step 2

What the user **has or is**
(2nd Authentication) such as:

- Their cell phone receiving a randomized alpha a/o numeric code in a text or email
- A mobile authentication app
- A security token providing a randomized alpha a/o numeric code

Authentication methods are based on principles that each one is independent of the other.



Basis of Authentication Methods

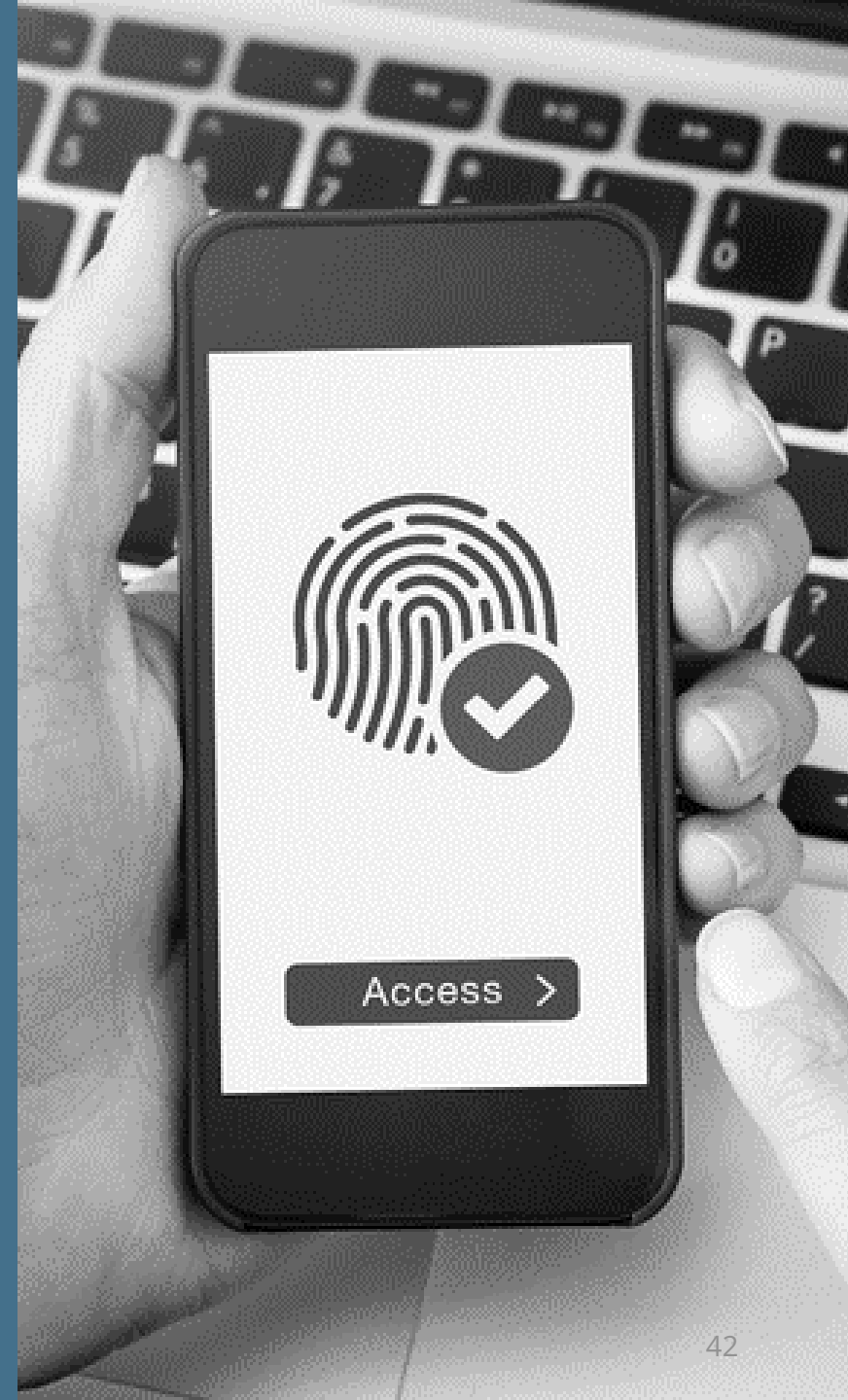
Step 2

(Continued)

What the user **has or is**
(2nd Authentication) such as:

- Biometric authentication:
 - Fingerprint verification
 - Voice print identification

Authentication methods are based on principles that each one is independent of the other.



Key Qualifiers

- ☐ Identify what you need to protect, and what form of attack would be successful in breaching it – does MFA stop it?
- ☐ Where in the process, or for what systems, are the risk factors sufficient to warrant it?
- ☐ If multiple systems are to be protected, on-premises and cloud-based, can one solution integrate with all of them?
- ☐ What is the system access/recovery plan if the MFA system fails or is offline?
- ☐ Do you have the resources required to evaluate, acquire, deploy and maintain the solution?



Save this **checklist** for later.

Key Solutions Consideration

- ☐ Is MFA already available in or for the system or application(s) in question?
- ☐ Does the MFA solution work for all users in consideration?
- ☐ Are the MFA solution options practical/useable by the users?
- ☐ Can SSO (Single Sign-On) be used to access multiple systems, in combination with MFA?
- ☐ Can a self-provisioning system meet your “Zero Trust” goals?
- ☐ If you allow BYOD, will the solution support all of the possible types and combinations of devices, and give equal telemetry and control over all of them?



Save this **checklist** for later.

Key Solutions Consideration: Advanced



Save this **checklist** for later.

- ☐ Does the solution have a flexible policy management method:
 - ☐ Different identity types, devices, etc.
 - ☐ Different community of user types
 - ☐ Workable or customizable authentication process flow
- ☐ Does the solution provide:
 - ☐ Adequate violation notifications
 - ☐ Reporting and logs to identify nefarious systemic activity or suspect access attempts
 - ☐ A dashboard for a live view of all users and connected devices
- ☐ If you have a SIEM (Security Information and Event Management system), will it export logs for that system?
- ☐ Does it integrate with your MDM, EDR, IDS, IPS, etc., system?

Key Solutions Consideration: Advanced

- ☐ An on-premises or cloud-based solution?
- ☐ Can the solution be interfaced or integrated without the need to replace or modify the target system or application?
- ☐ What is the API (Application Programming Interface) availability for integration with the system or application?
- ☐ Does the solution employ:
 - ☐ Behaviour Analytics
 - ☐ Device Trust and Health Check
 - ☐ Device Flexibility



Save this **checklist** for later.

Standards: Advanced

- ☐ Beware of and consider open standards for authentication and secure communications such as FIDO2 (WebAuthn+CTAP2), SAML, OpenID Connect, OAuth2, TLS, etc.
- ☐ Ensure any cloud-based solution provider is SOC II audited a/o ISO 27001 certified
- ☐ Ensure the use of biometrics and collection of location data, etc., is in compliance with the Privacy Act and other regulatory requirements



Save this **checklist** for later.



[Go Back](#)