Enhancing Password Security and the Power of Multi-Factor Authentication

NPC Safe Computing Webinar Series

January 18th, 2022

Larry Keating, President
Darren Mar, National Sales Manager

NPC

Thank You!

ALIGNED capital partners inc.

MFDA Mutual Fund Dealers Association of Canada
Association canadienne des courtiers de fonds mutuels

PPI Solutions

Manulife Securities

Advocis The Financial Advisors Association of Canada

MANDEVILLE PRIVATE CLIENT INC.

FaithLife® FINANCIAL

AON

Investment Planning Counsel®
IPC VALEURS MOBILIÈRES

GROVE POINT FINANCIAL

HollisWealth

IDC WORLDSOURCE INSURANCE NETWORK INC.

Advisor Research Group Inc.

CI FINANCIAL

IIAC ACCVM
INVESTMENT INDUSTRY ASSOCIATION OF CANADA
ASSOCIATION CANADIENNE DU COMMERCE DES VALEURS MOBILIÈRES

FINANCIAL LITERACY COUNSEL INC.

GLOBAL MAXFIN INVESTMENTS INC.

EQUITY Associates Inc.

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
- Q&A

Passwords and Passphrases

Common Misconceptions

The banks only ask for an eight character password, so it must be good 👎

Replacing letters with digits or symbols makes it OK to use a shorter password 👎

- Like a “$” for “5” or a “3” for an “E”

Using a string of symbols or character gobbledegook, like $#%#@ makes it OK to use a shorter password 👎

When there are only three attempts you can try, a simpler password is OK 👎

You should never write your passwords down 👎

REALLY?!

Some Password Truths

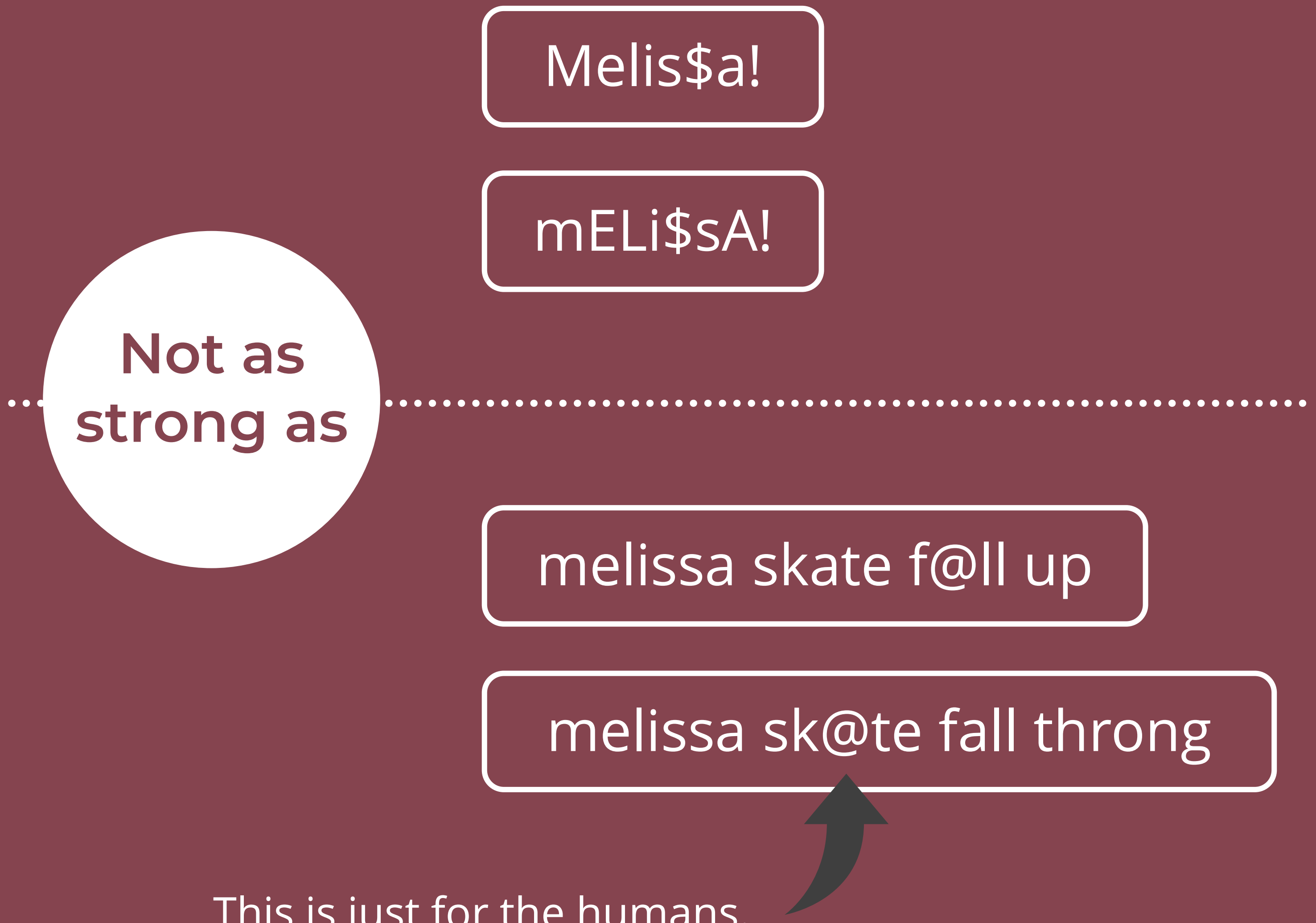
- We’ve made passwords easy for computers to guess, but hard for people to remember (or type)
- We try to create “entropy” –increased difficulty for the computer to guess – by making things appear scrambled
- And the more scrambled, the harder it is for a human to type or remember
- So, people use simpler, shorter passwords, or reuse them, weakening password security
- But a computer processes information and makes calculations different than a human
- What looks scrambled to us, may not be a challenge for the computer

Passwords and Passphrases

Favour **length** over complexity.

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

Try to use one **uncommon** word.



Melis$a!

mELi$sA!

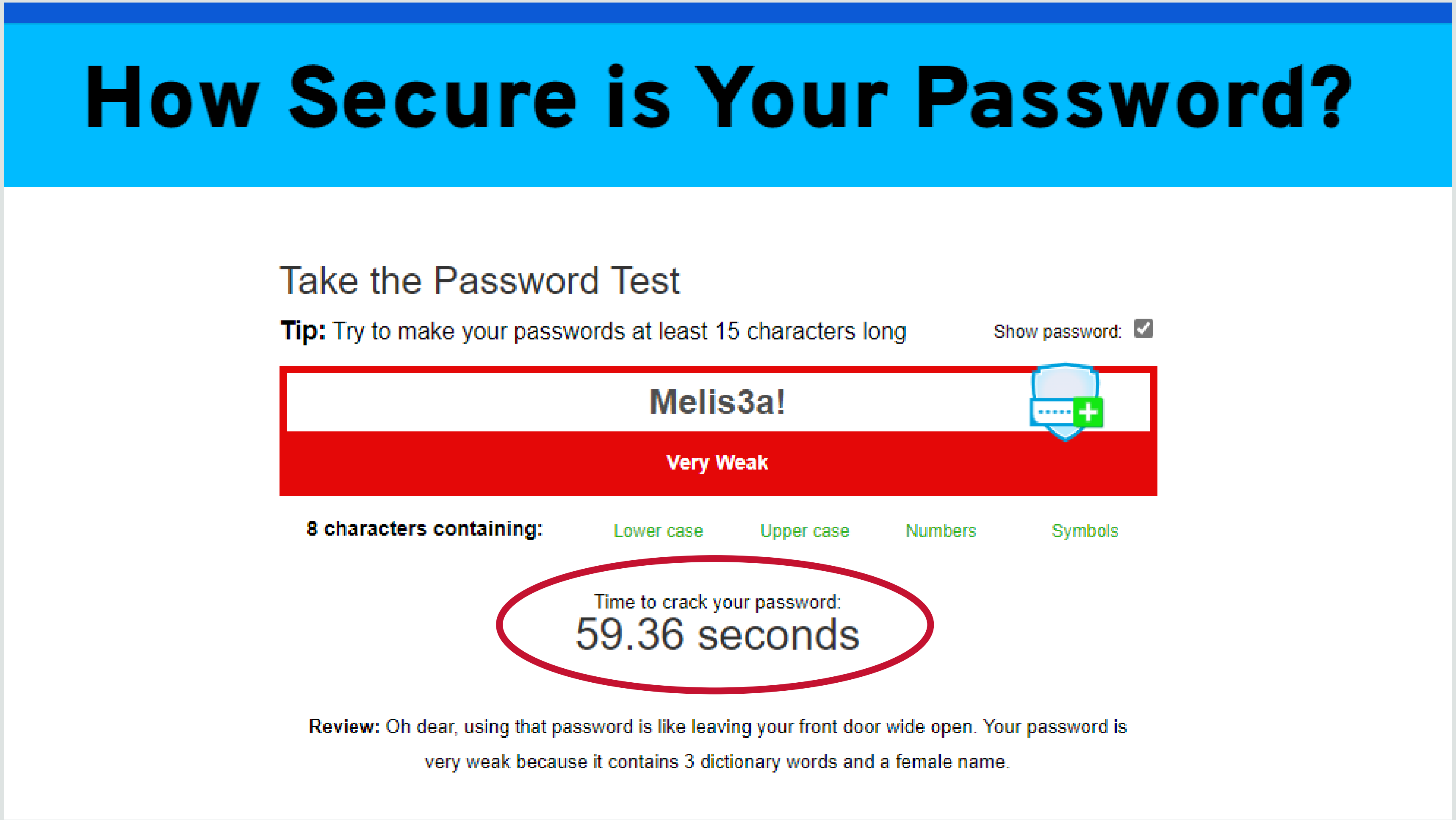
Not as strong as

melissa skate f@ll up

melissa sk@te fall throng

This is just for the humans.

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

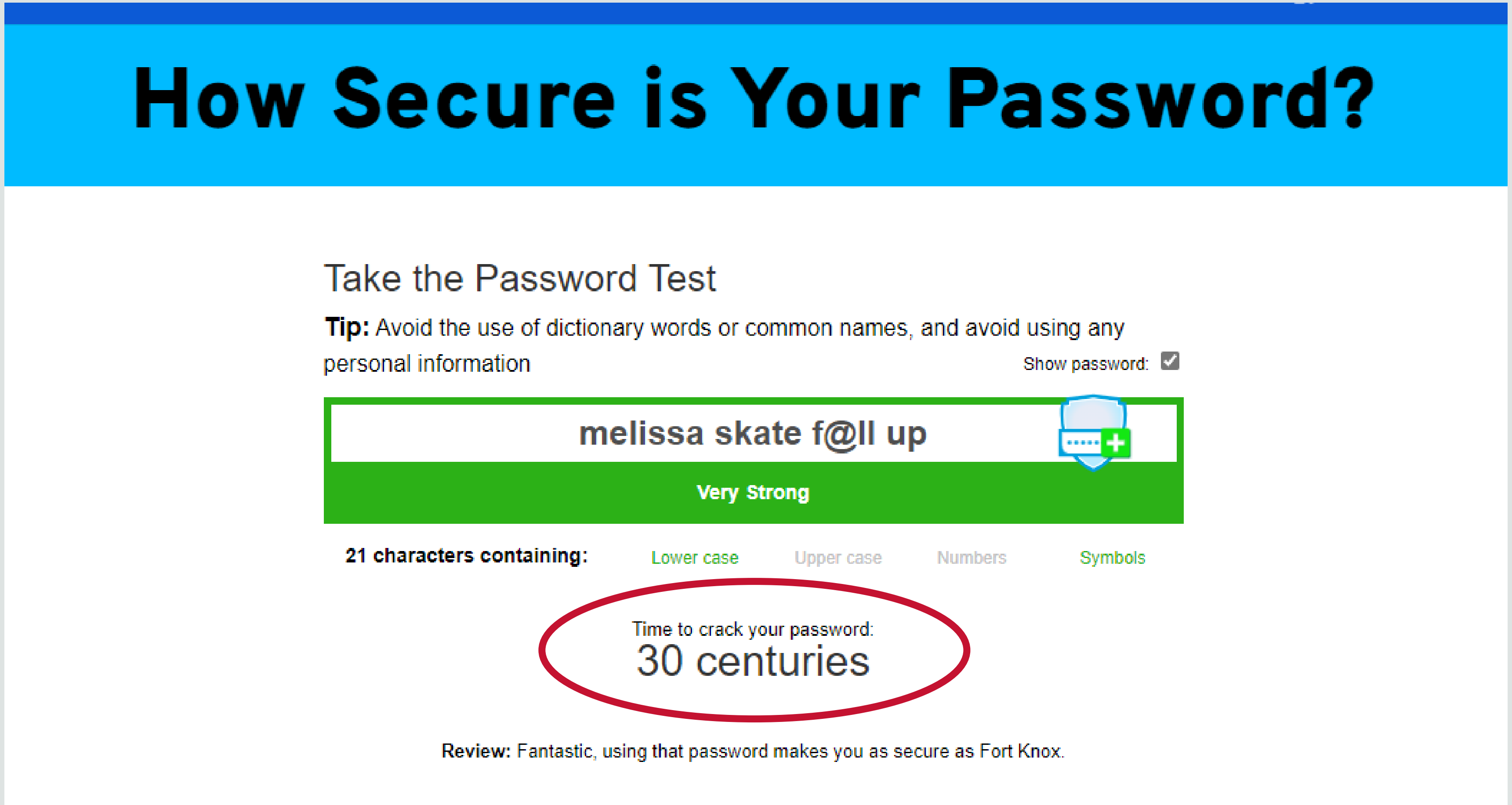
8 characters containing: Lower case Upper case Numbers Symbols

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.

Source: My1Login.com

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

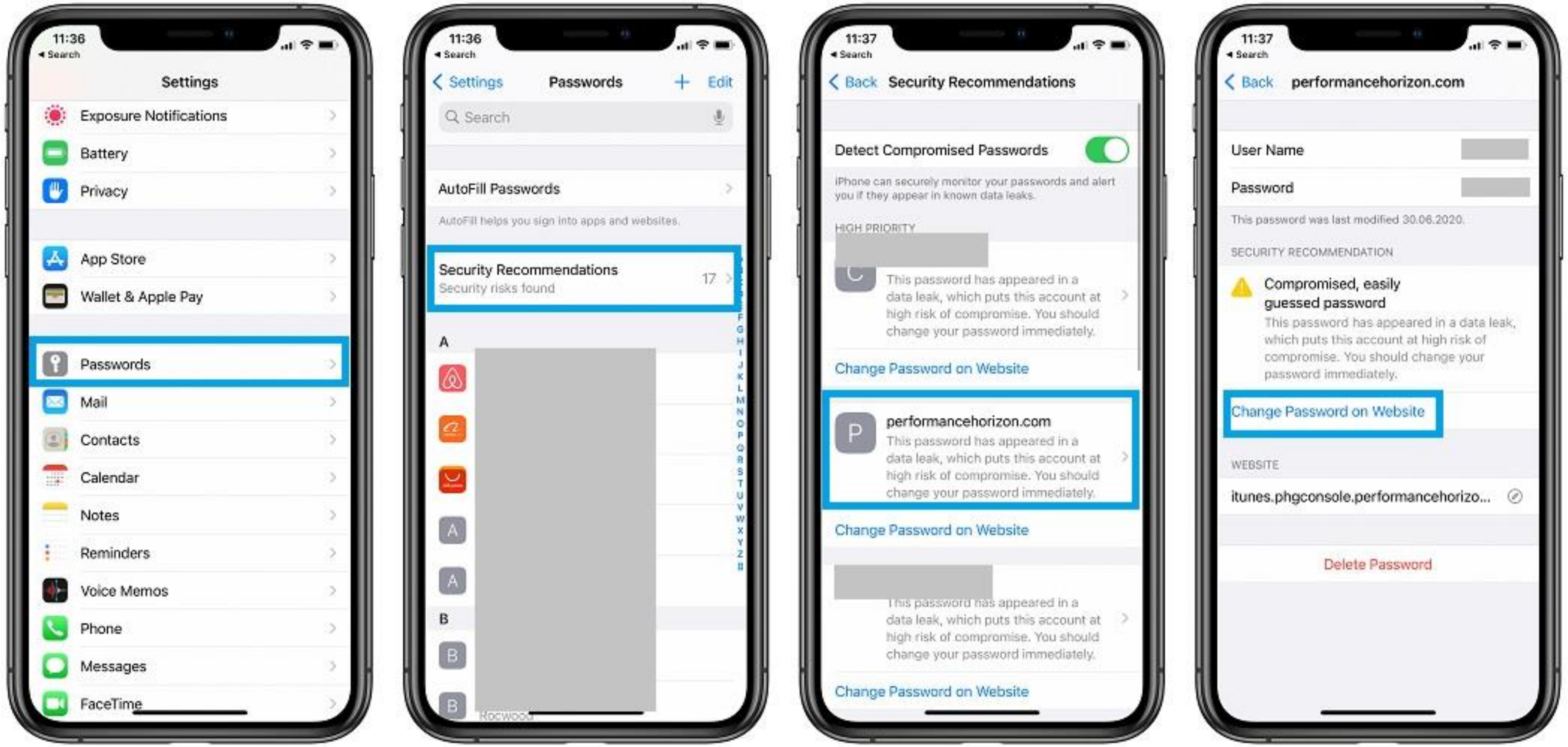
21 characters containing: Lower case Upper case Numbers Symbols

Time to crack your password:
30 centuries

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

Source: My1Login.com

Passwords Security Recommendations



11:36
◂ Search

Settings

Exposure Notifications

Battery

Privacy

App Store

Wallet & Apple Pay

Passwords

Mail

Contacts

Calendar

Notes

Reminders

Voice Memos

Phone

Messages

FaceTime

11:36
◂ Search

< Settings Passwords + Edit

Search

AutoFill Passwords

AutoFill helps you sign into apps and websites.

Security Recommendations 17
Security risks found

A

[redacted]

B

11:37
◂ Search

< Back Security Recommendations

Detect Compromised Passwords

iPhone can securely monitor your passwords and alert you if they appear in known data leaks.

HIGH PRIORITY

[redacted]

This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.

Change Password on Website

performancehorizon.com
This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.

Change Password on Website

[redacted]

This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.

Change Password on Website

11:37
◂ Search

< Back performancehorizon.com

User Name [redacted]

Password [redacted]

This password was last modified 30.06.2020.

SECURITY RECOMMENDATION

Compromised, easily guessed password
This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.

Change Password on Website

WEBSITE

itunes.phgconsole.performancehorizo...

Delete Password

Source: iPhone Compromised Password Notification (Fact Or Hack?) (iphonetricks.org)

Passwords and Passphrases Best Practices

❑ Use passphrases, favour length over complexity

❑ Change your passwords regularly – every 90 - 120 days

❑ Never text or email a password with the login name

❑ 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

❑ Never embed personal info in your browser

Save this **checklist** for later.

Passwords and Passphrases Best Practices

☑ Save this **checklist** for later.

- ❑ Use fingerprint readers
  - Allows longer passwords and passphrases, without the inconvenience of having to frequently type them
- ❑ Use two-factor / multi-factor authentication
- ❑ 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
- ❑ Online password managers that centralize all your passwords should be very carefully researched and considered

Writing Passwords Down

Save this **checklist** for later.

- ❑ 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:

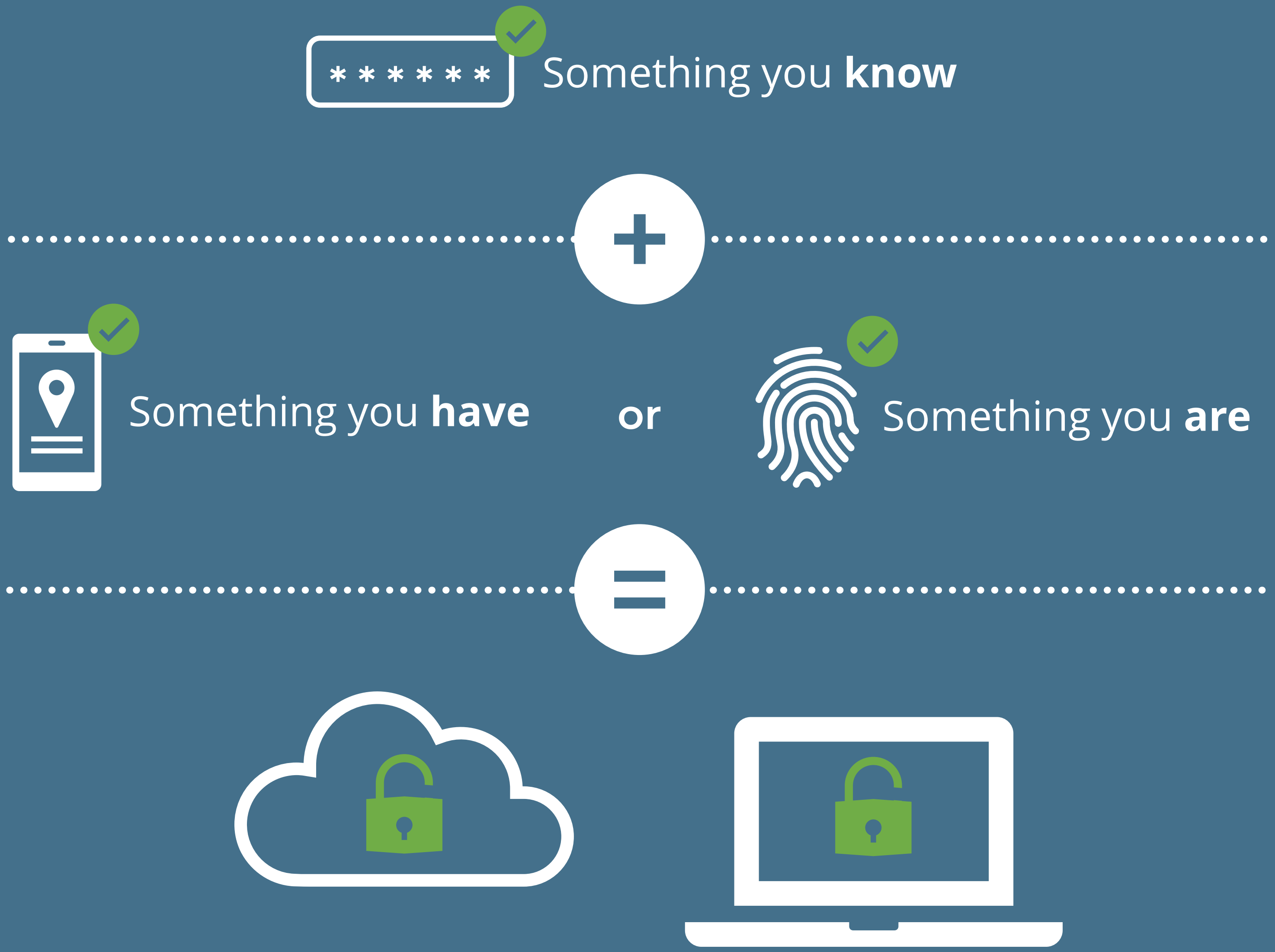
- ❑ Be absolutely certain that how you are storing and managing it is secure
- ❑ Do not write down the associated usernames or site/services they are for. But know that for most of your logins it is your email address, and that is known
- ❑ Change them slightly, but do not make the change uniform

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.



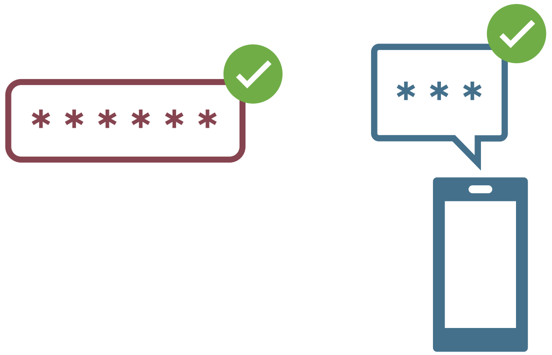
Something you **know**

+

Something you **have** **or** Something you **are**

=

Multi-Factor Authentication Definitions

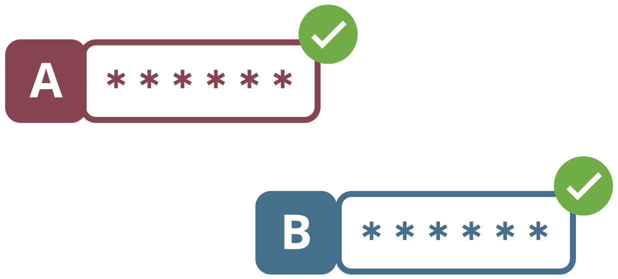


2FA: Two-Factor Authentication

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.

⚠ Not a fan of this option

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

August 27, 2019

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

Source: Microsoft: Using multi-factor authentication blocks 99.9% of account hacks | ZDNet

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

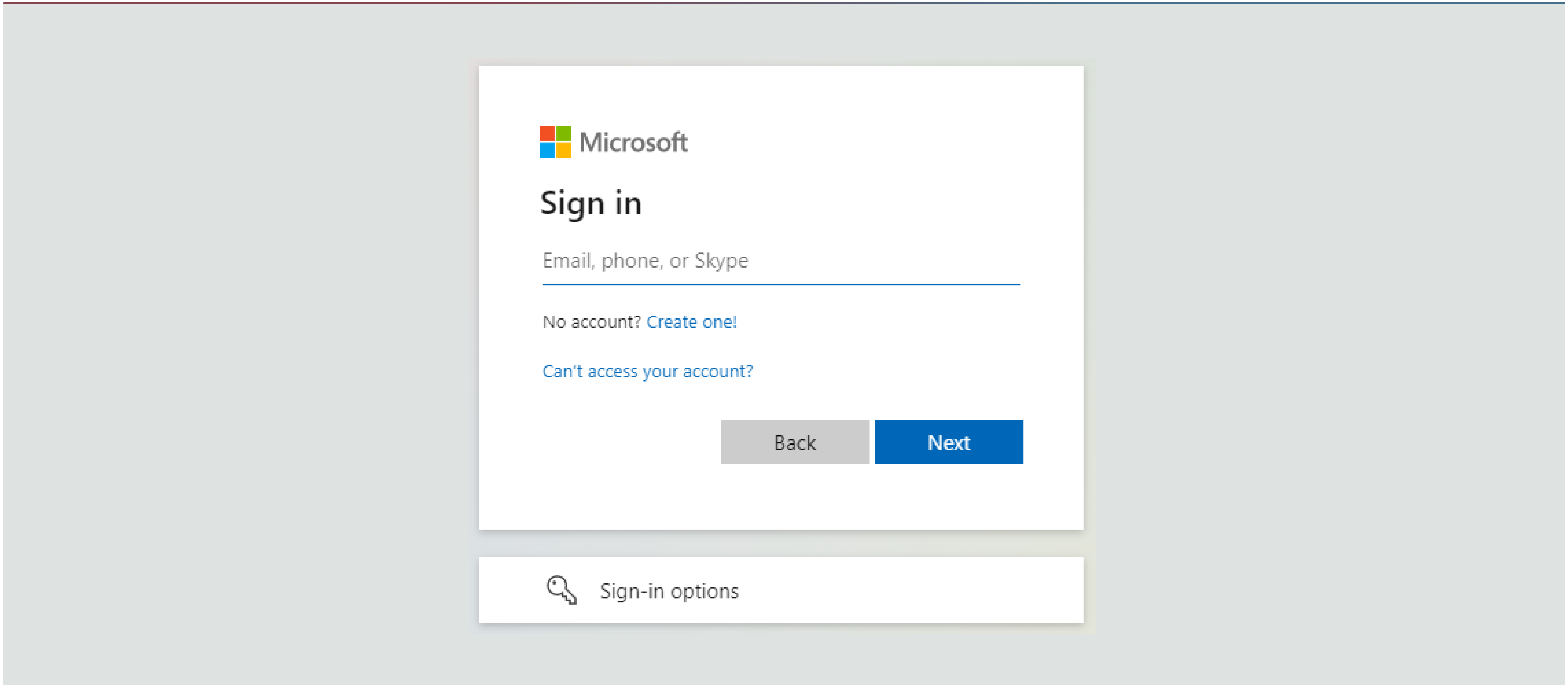
Credential Stuffing

Keyloggers

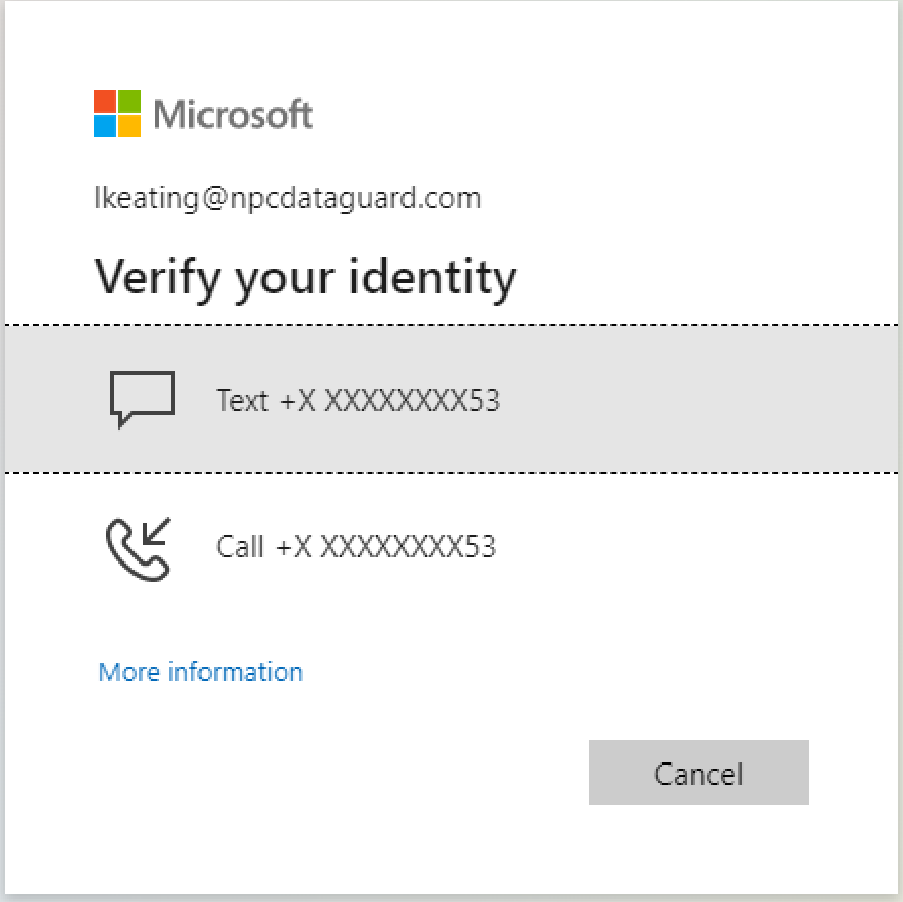
Reverse Brute-Force Attacks

Brute-Force Attacks

Microsoft 365 MFA



Microsoft 365 MFA

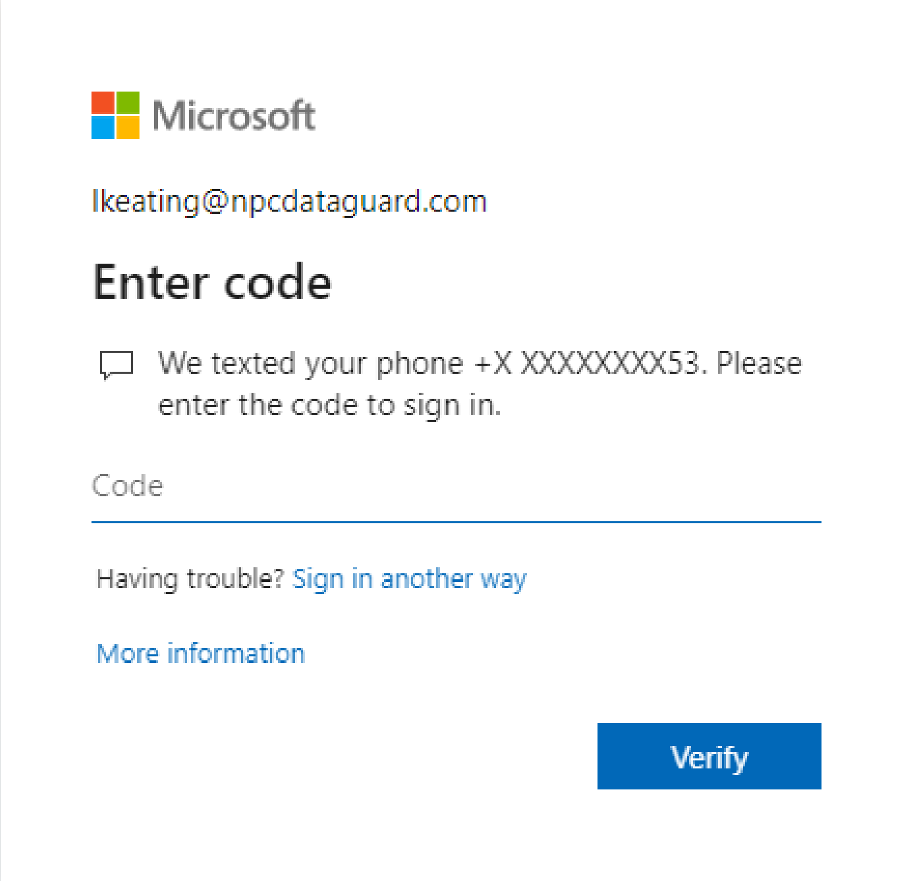


Microsoft

lkeating@npcdataguard.com

Verify your identity

Microsoft 365 MFA



Microsoft

lkeating@npcdataguard.com

Enter code

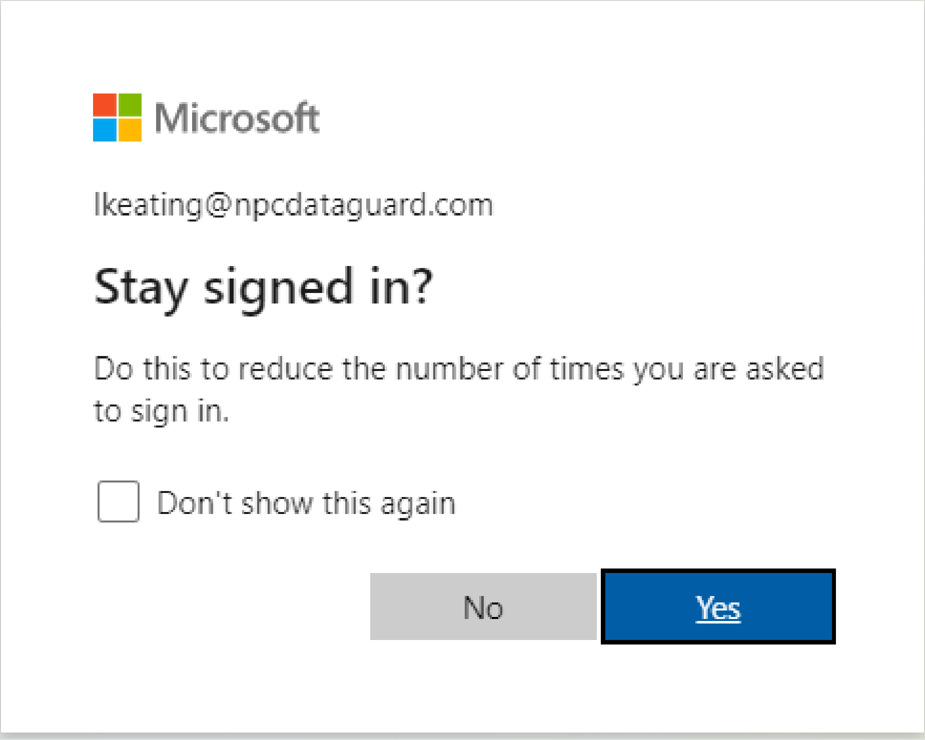
We texted your phone +X XXXXXXXX53. Please enter the code to sign in.

Code

Having trouble? Sign in another way

More information

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.

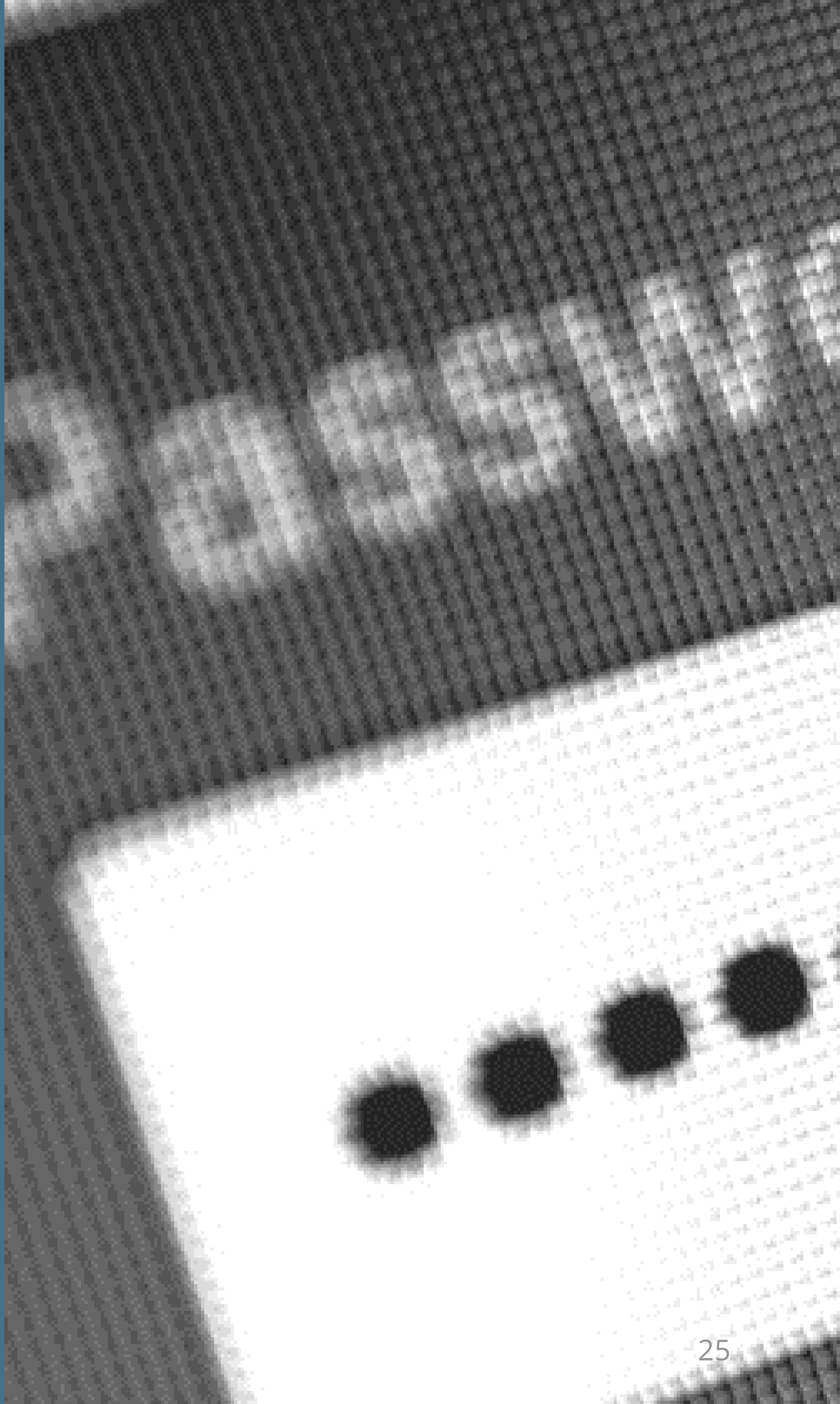
Basis of Authentication Methods

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.



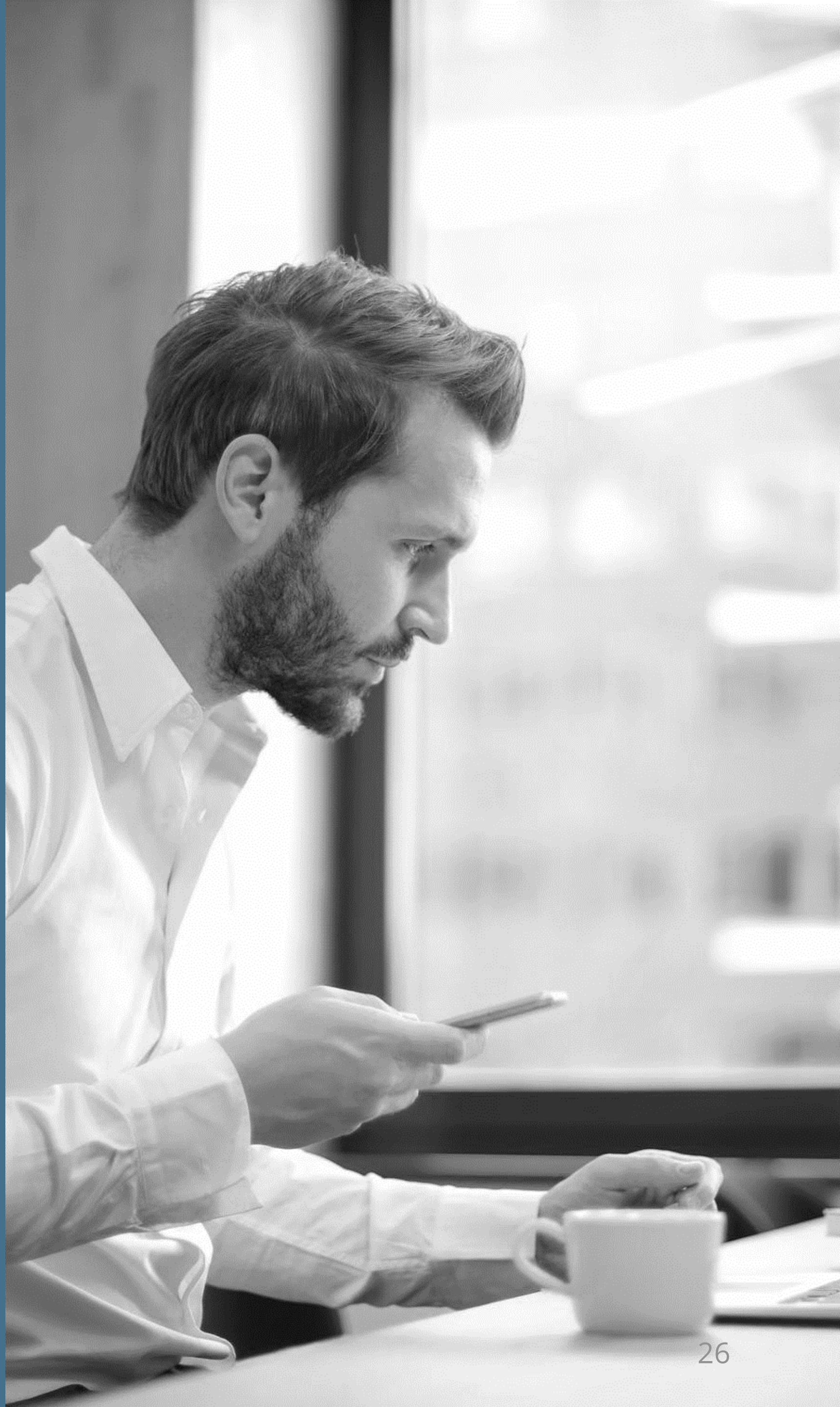
Basis of Authentication Methods

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

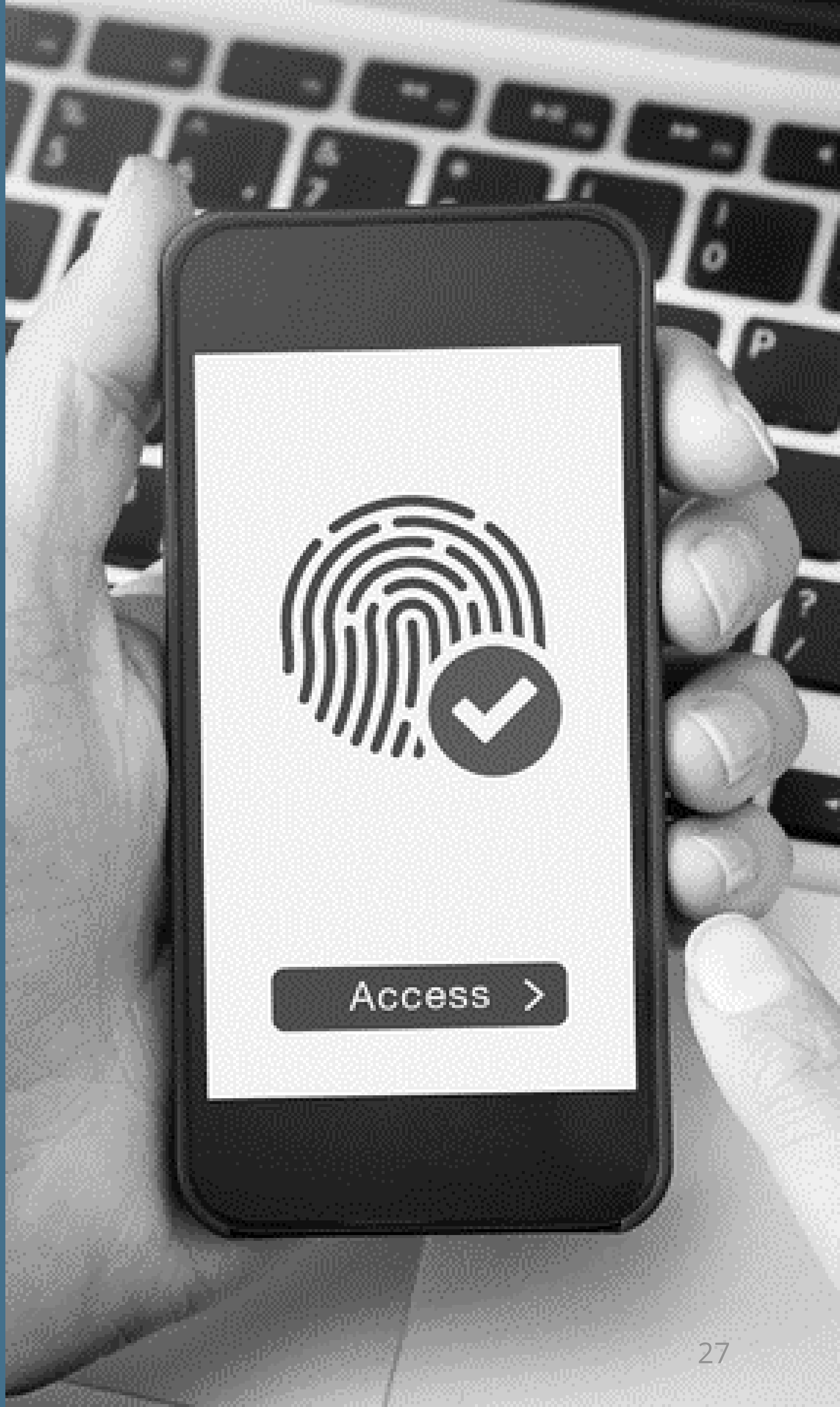
Step
2

(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.



Basis of Authentication Methods

Go to **Implementation**

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

Additional Resources

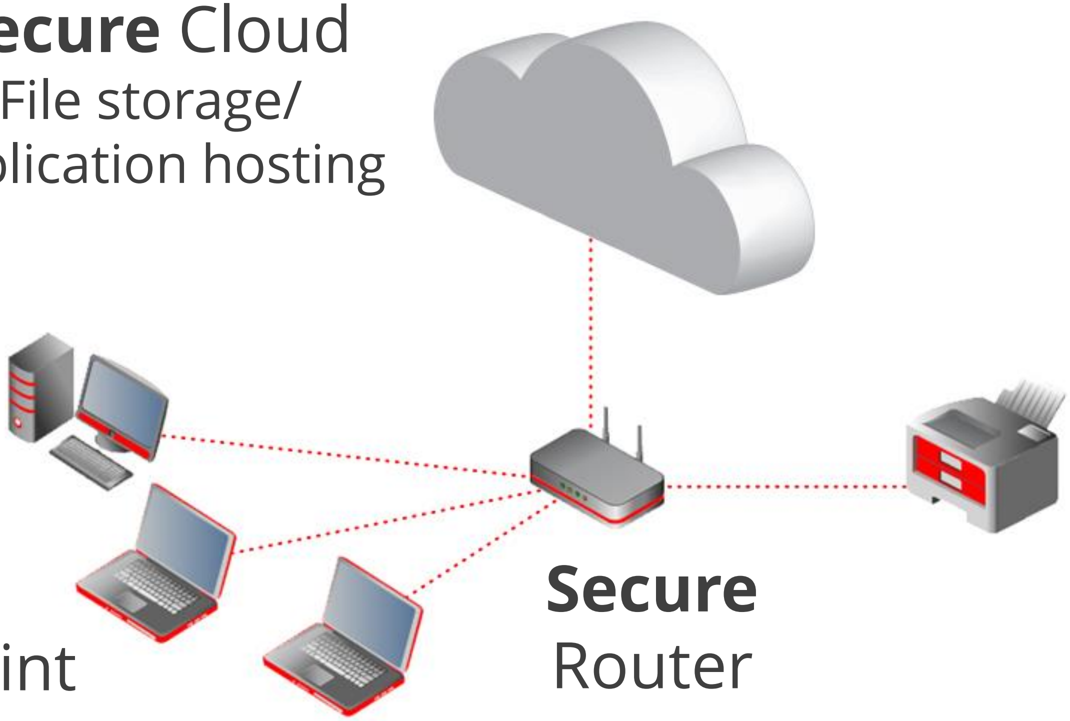
NPC Solutions

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

www.npcdataguard.com

- NPC Secure Managed Computers
  - Managed hardware, encryption, backup, system software, security, technical support and insurance
- NPC Managed Microsoft Office 365
  - SharePoint for advanced file storage and sharing, Exchange Email, Teams, and a host of productivity tools
- Dedicated Account Manager
  - A custom and consultative approach

Office of the Future



Secure Cloud
File storage/
application hosting

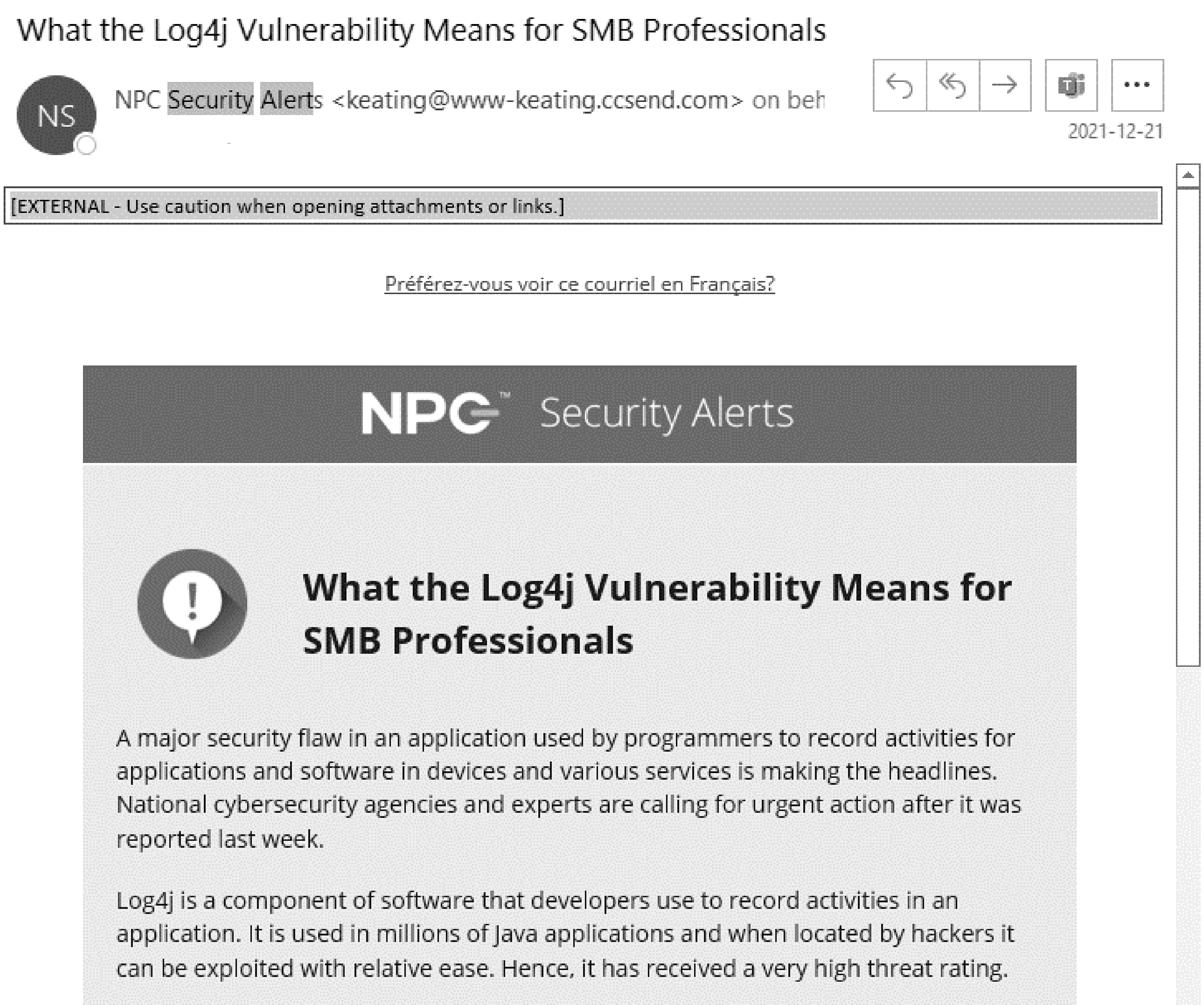
Secure Printer,
Copier, Scanner

Secure
Router

Secure Endpoint
Devices

NPC Security Alerts

npcdataguard.com/alerts



What the Log4j Vulnerability Means for SMB Professionals

NPC Security Alerts <keating@www-keating.ccsend.com> on beh

2021-12-21

[EXTERNAL - Use caution when opening attachments or links.]

Préférez-vous voir ce courriel en Français?

NPC Security Alerts

What the Log4j Vulnerability Means for SMB Professionals

A major security flaw in an application used by programmers to record activities for applications and software in devices and various services is making the headlines. National cybersecurity agencies and experts are calling for urgent action after it was reported last week.

Log4j is a component of software that developers use to record activities in an application. It is used in millions of Java applications and when located by hackers it can be exploited with relative ease. Hence, it has received a very high threat rating.

Upcoming NPC Webinars

→ npcdataguard.com/webinars

January 20th 1pm ET (30-minute)	NPC DataGuard Solutions Overview
February 15th 1pm ET (60-minute)	Microsoft 365 Basics for Secure Remote Work
February 17th 1pm ET (30-minute)	NPC DataGuard Solutions Overview

NPC Webinars Recordings

→ npcdataguard.com/webinars

Securing Your Business from Ransomware and Business Email Compromise

Building an Incident Response Plan for the SMB

Five Critical Requirements for Work From Home or Small Office Computers

Protecting Your Identity Online

+ New Topics Will Be Added

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

NPC™

Smarter Computing

Multi-Factor Authentication Implementation Considerations

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

- ❑ 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?

Save this **checklist** for later.

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**