PNI HCM

GovConPay
Focus Matters

Cybersecurity

Threats Facing Organizations Today

July 23, 2025

Housekeeping Items

Before We Get Started

A recording of this webinar will be sent to you after today’s presentation.

Housekeeping Items

Before We Get Started

All attendees will be placed on mute.

Please place questions in the chat tab.

A survey will be sent out after the webinar.

Housekeeping Items

If you’re having trouble with audio or viewing the webinar, please:

- Try refreshing your browser.
- Try a different browser.
- Ask for assistance in the chat tab.

Meet Your Presenters

Nick Holcomb

Chief Technology Officer
PNI•HCM & GovConPay

Amy Miller

VP of Training
PNI•HCM & GovConPay

Our Agenda

- Understanding Phishing
- Navigating Fake Websites
- Reviewing Password Security
- Implementing Modern Authentication
- Defining the Principle of Least Privilege
- Using isolved

PNI HCM

GovConPay
Focus Matters

Polling Question

How often do you provide Security Training to your employees?

*Polls will appear above the chat window.

Phishing

Prevalent Threat

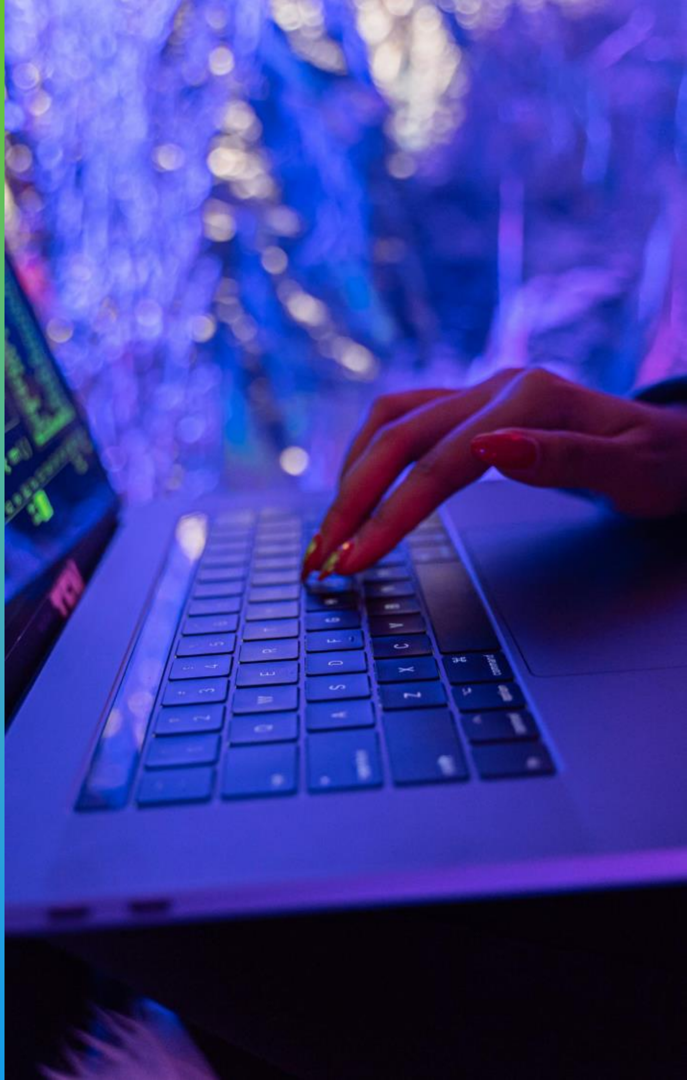
Phishing is a widespread threat affecting organizations, often targeting employees to extract sensitive information.

Recognizing Phishing Attempts

Understanding how to identify phishing attempts is essential for protecting sensitive company data from breaches.

Safeguarding Data

Implementing security measures and employee training can significantly reduce the risk of falling victim to phishing.



Spear-Phishing

Targeting individuals to log in to fraudulent websites.

Steps to The Targeted Tactics

Information Gathering (Bait)

The Request (The Hook)

The Attack (Catch)

Implementing Phishing Awareness Programs

Employee Education

Training Sessions

Simulations & Drills

Phish Alert Tools

Clear Instructions & Support

Navigating Fake Websites

Understanding Fake Websites

What are they?

Why do they exist?

How do they operate?

Can you spot a fake website?

ANALYZE THE URL

CHECK FOR CONTACT INFORMATION

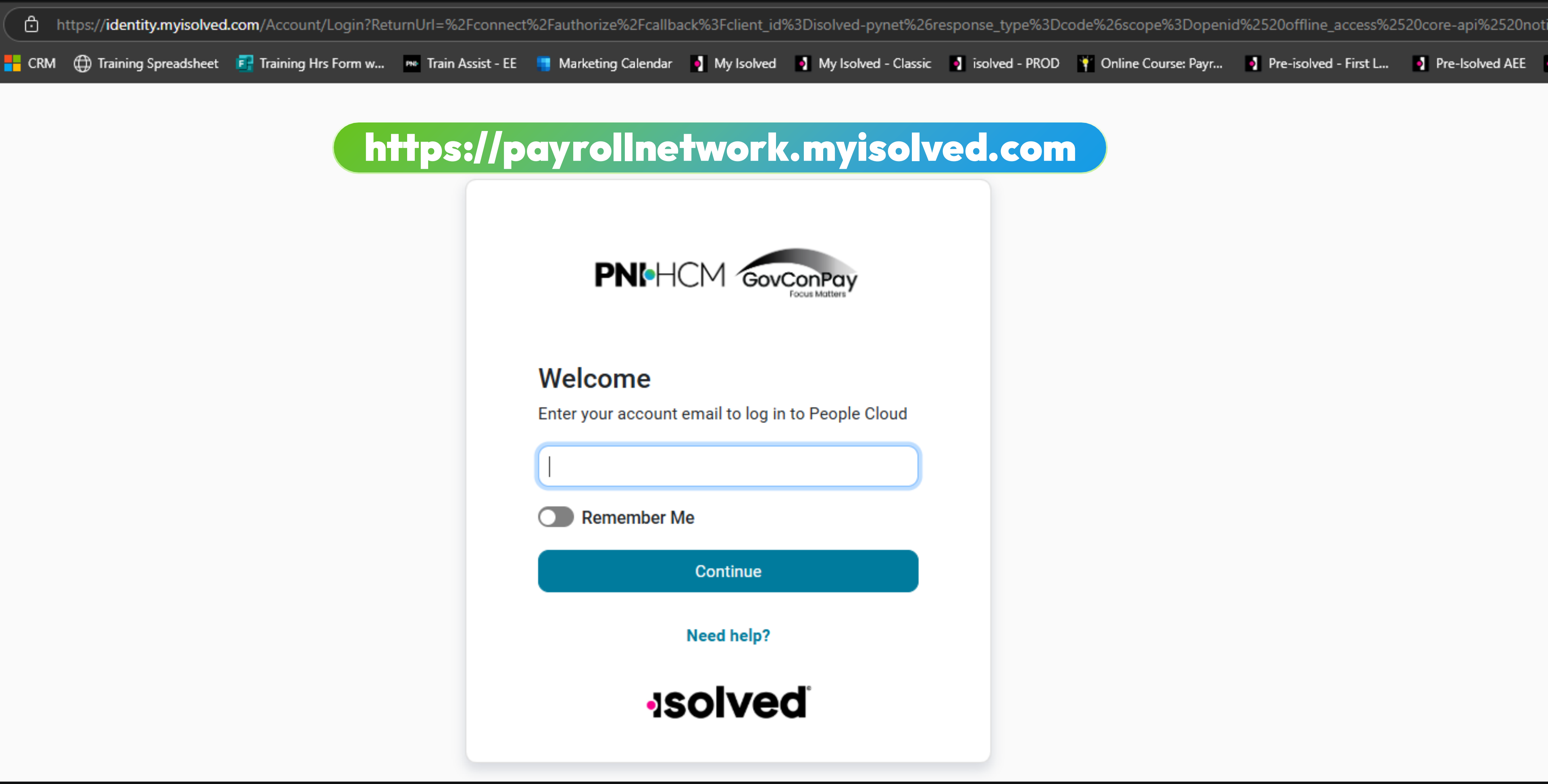
EVALUATE THE WEBSITE DESIGN AND CONTENT

TEST THE WEBSITE FUNCTIONALITY

Keeping You Safe

- ☐ Educate Employees on Security
- ☐ Provide Links & Favorites (Avoid using search engines.)
- ☐ Use Official App Stores
- ☐ Enable Modern Authentication
- ☐ Review Email & Domain Names for Accuracy
- ☐ Review Authorized Contacts with PNI
- ☐ Avoid Sending PII Information via Email
- ☐ Preview Your Payroll for Verification of Changes
- ☐ Review Your Account for Accuracy (Employee)

https://payrollnetwork.myisolved.com



https://identity.myisolved.com/Account/Login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3Disolved-pynet%26response_type%3Dcode%26scope%3Dopenid%2520offline_access%2520core-api%2520noti

Welcome

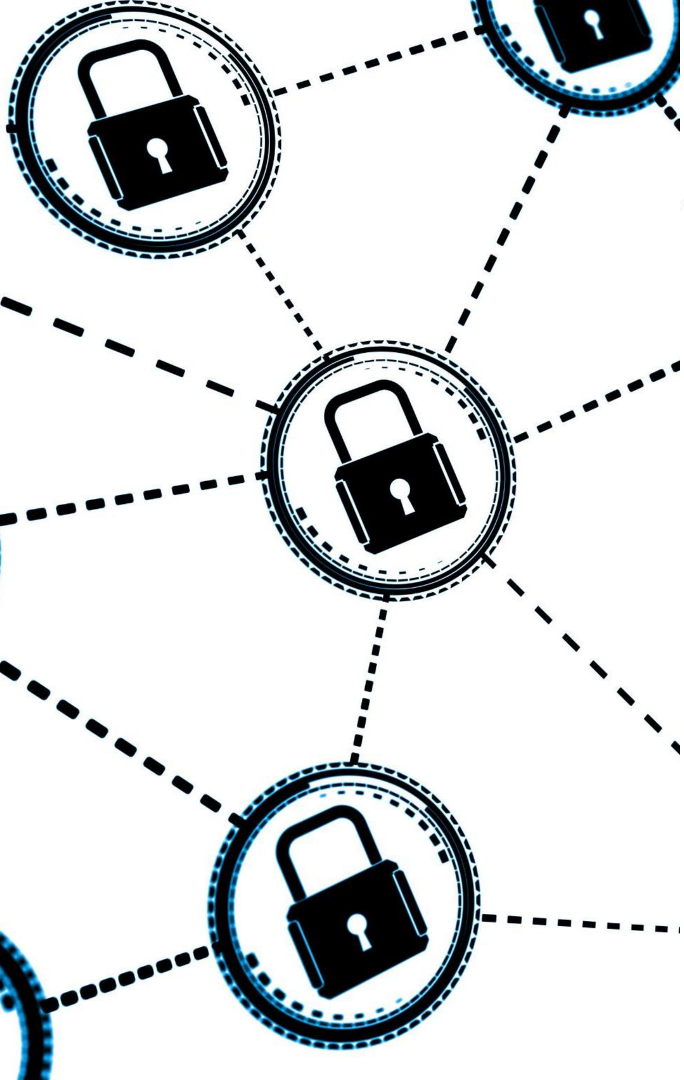
Enter your account email to log in to People Cloud

Remember Me

Polling Question

True or False:
Passwords are considered the safest in preventing breaches and attacks.

*Polls will appear above the chat window.



The Current Status on Passwords

Weakness of Passwords

Passwords are frequently the **most** vulnerable aspect of cybersecurity, making systems susceptible to breaches and attacks.

Rise of Breaches

As cybersecurity breaches continue to increase, reliance on traditional passwords poses significant risks for organizations.

Need for Alternatives

Organizations must explore alternative security measures beyond traditional passwords to protect sensitive information effectively.

Polling Question

Do you reuse the same password?

*Polls will appear above the chat window.

Go “Passwordless” & Use Passkeys

Enhanced Security
Passwordless authentication methods significantly improve security by eliminating the vulnerabilities associated with traditional passwords.

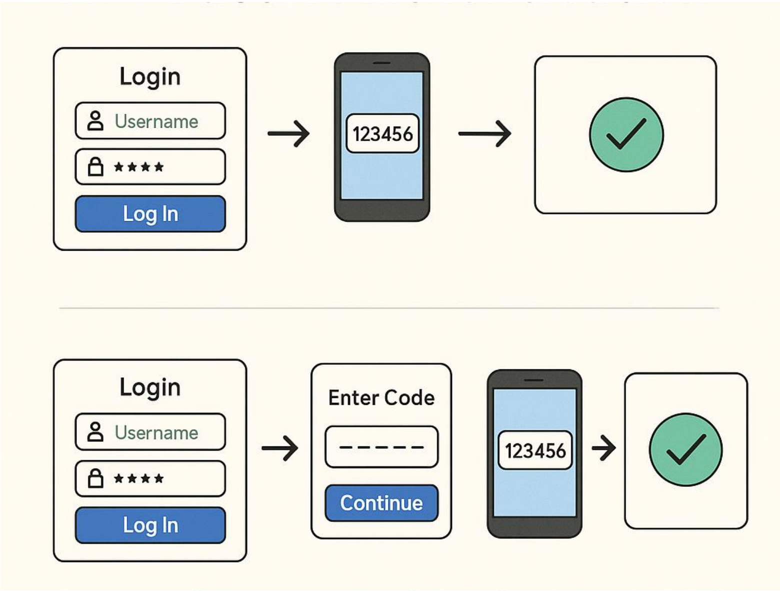
Simplified Login Process
Passkeys streamline the login process, making it faster and more user-friendly for accessing accounts.

Reduced Password Management Risks
By adopting passkeys, organizations can significantly reduce risks linked to password management, such as phishing attacks.

The Evolution of Multi-Factor Authentication

- Started with simple two-factor authentication (2FA) methods, such as combining a password with a one-time code sent via SMS or email.

- The need for more robust security led to the introduction of additional authentication factors, including passkey authentication, biometric verification (fingerprint, facial recognition) and hardware tokens.



Polling Question

Is Multi-Factor Authentication Secure?

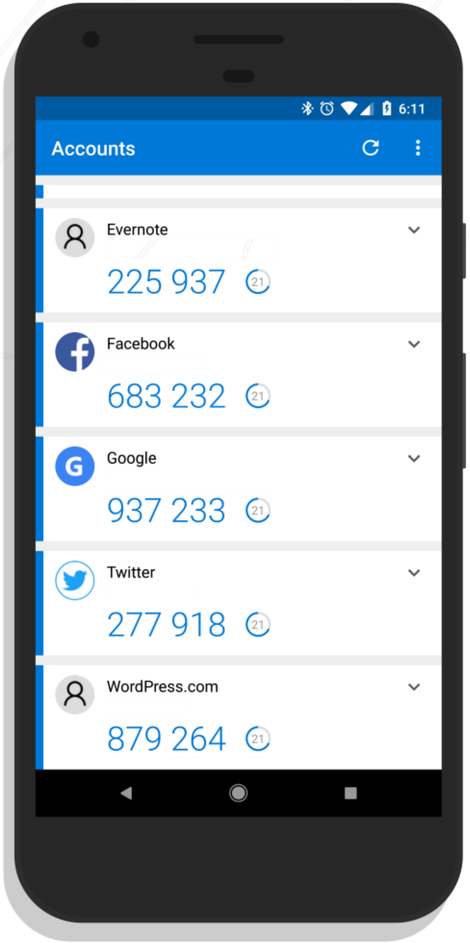
*Polls will appear above the chat window.

Email & Text-Based Authorization Codes Are Being Phased Out

Decreasing Reliance on Codes
The reliance on email and SMS codes for verification is decreasing due to increasing security vulnerabilities.

Security Vulnerabilities
Email and SMS codes are prone to vulnerabilities, making them less secure for authentication purposes.

Transition to Secure Methods
Organizations are encouraged to adopt more secure methods of verification to enhance user safety.



Evernote
225 937

Facebook
683 232

Google
937 233

Twitter
277 918

WordPress.com
879 264

Using Authenticator Apps

Enhanced Security

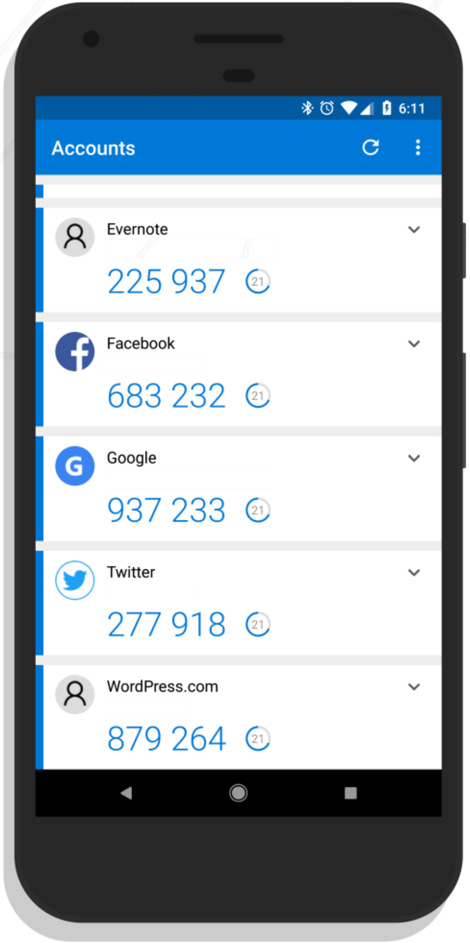
Authenticator apps are considered more secure than SMS 2FA because they store the secret key on the device itself, making it harder for hackers to intercept the codes

Convenience

Authenticator apps are easy to use and can be integrated with a wide range of online services, from social networks to financial services

Time-Based, One-Time Use Codes

The codes generated by authenticator apps are short-lived, usually expiring within 30 seconds. This minimizes the window of opportunity for potential attackers



Accounts

Evernote
225 937 (21)

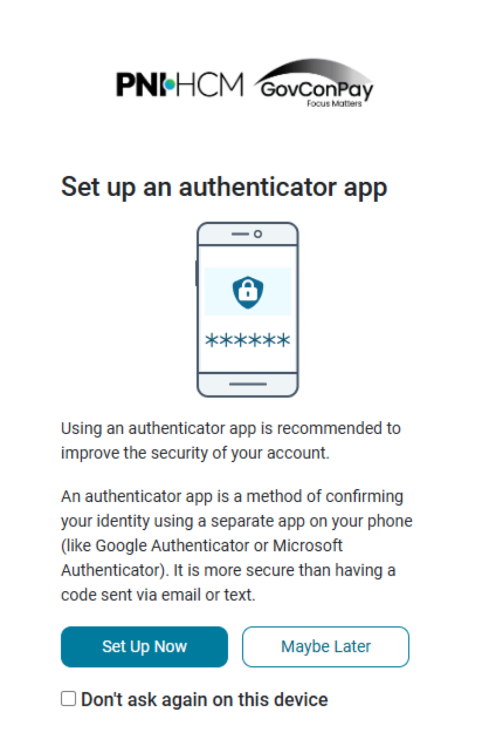
Facebook
683 232 (21)

Google
937 233 (21)

Twitter
277 918 (21)

WordPress.com
879 264 (21)

Using Authenticator Apps



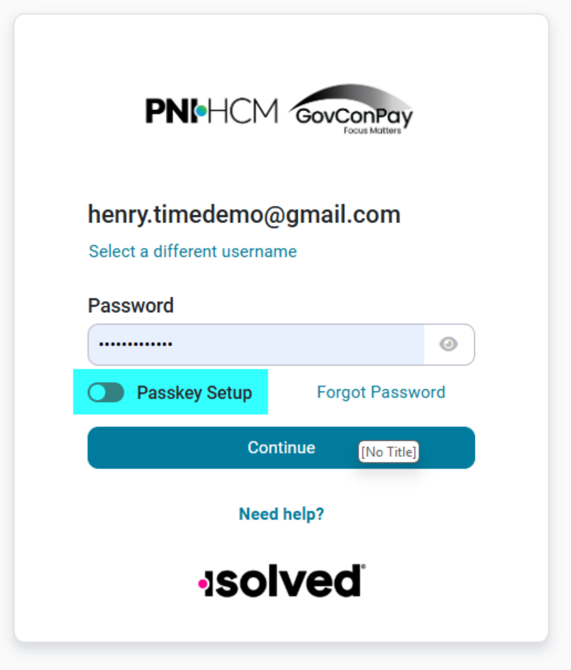
Set up an authenticator app

Using an authenticator app is recommended to improve the security of your account.

An authenticator app is a method of confirming your identity using a separate app on your phone (like Google Authenticator or Microsoft Authenticator). It is more secure than having a code sent via email or text.

□ Don't ask again on this device

Utilizing Passkeys

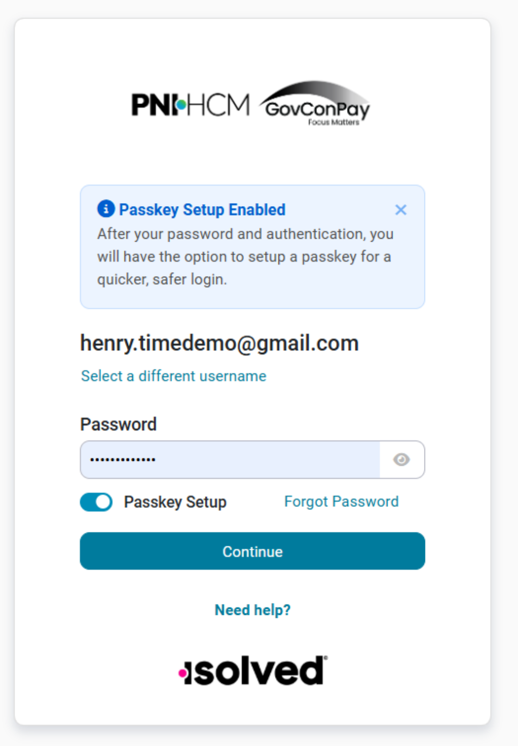


henry.timedemo@gmail.com

Select a different username

Password

••••••••••••••



Passkey Setup Enabled

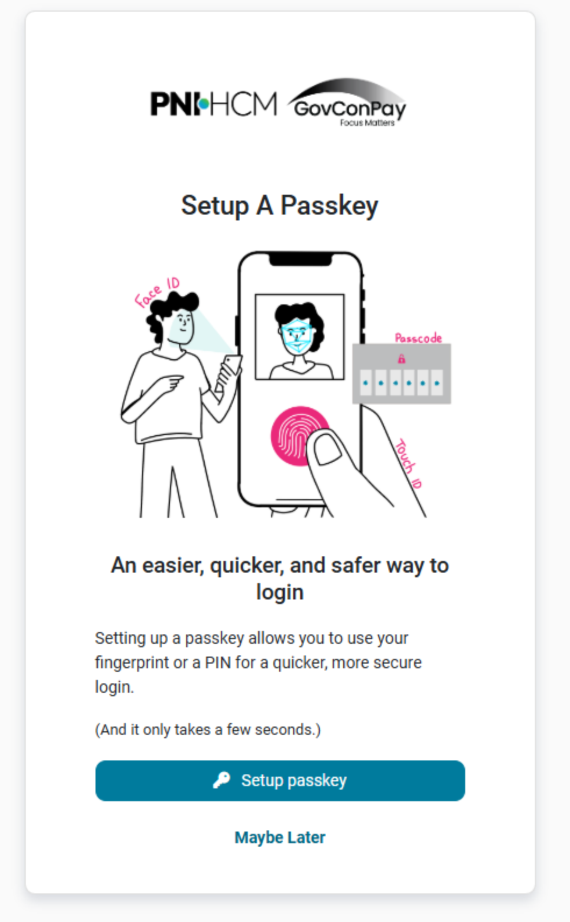
After your password and authentication, you will have the option to setup a passkey for a quicker, safer login.

henry.timedemo@gmail.com

Select a different username

Password

••••••••••••••



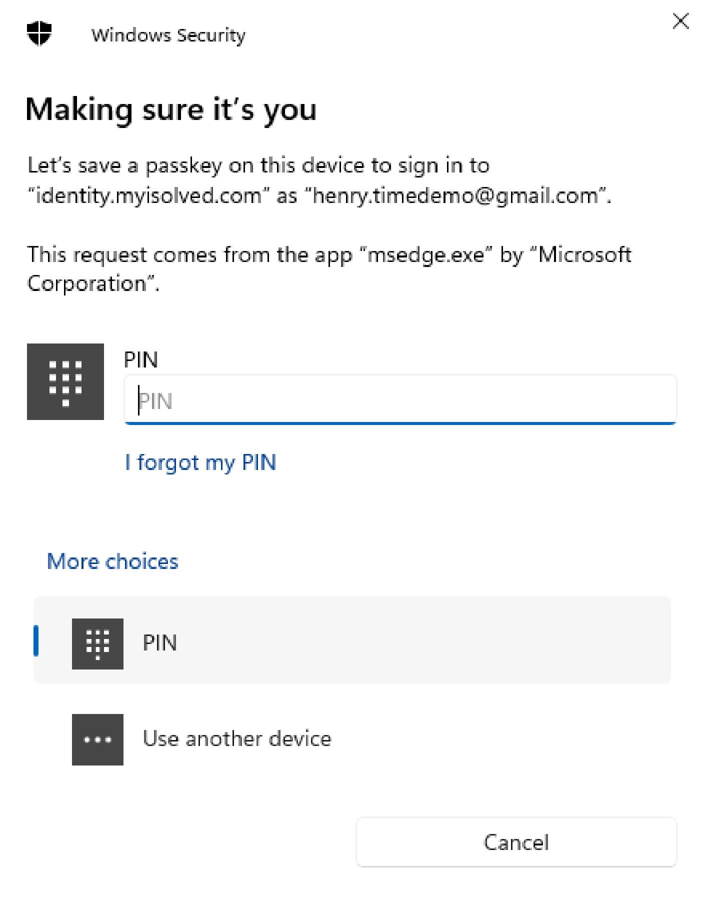
Setup A Passkey

An easier, quicker, and safer way to login

Setting up a passkey allows you to use your fingerprint or a PIN for a quicker, more secure login.

(And it only takes a few seconds.)

Utilizing Passkeys



Making sure it's you

Let's save a passkey on this device to sign in to "identity.myisolved.com" as "henry.timedemo@gmail.com".

This request comes from the app "msedge.exe" by "Microsoft Corporation".

PIN: PIN

Polling Question

Do you have an incident response plan in place?

*Polls will appear above the chat window.

What’s your plan?

- ❑ Identifying Threats
- ❑ Defining a Response Team
- ❑ Outlining Procedures
- ❑ Developing a Communication Plan
- ❑ Testing & Updating the Plan
- ❑ Training All Stakeholders/Employees

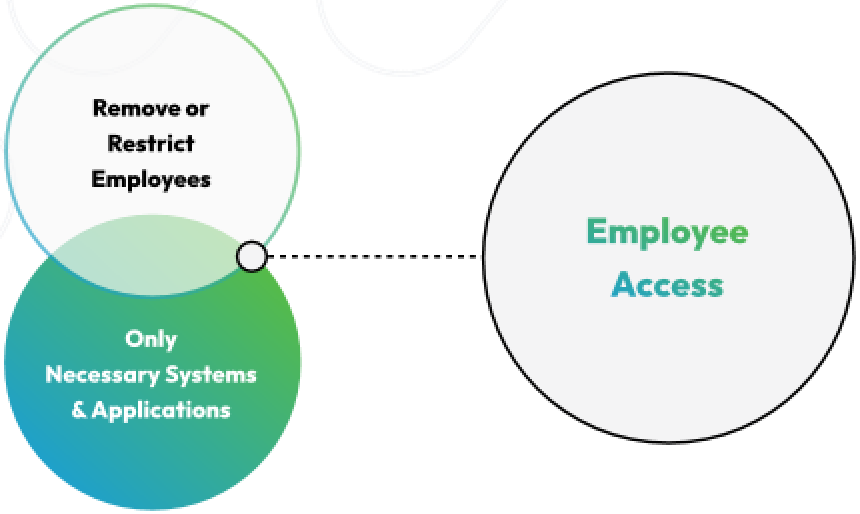
Principle of Least Privilege (PoLP)

Minimizing Access

Reduce Risks

User Access Management

PoLP – Principle of Least Privilege


Remove or Restrict Employees
Only Necessary Systems & Applications
Employee Access

- **Identify Sensitive Data**

  Understand the need for crucial access.

- **Perform Regular Access Reviews**

  Identify and correct user permissions.

- **Compliance Assurance**

  Ensure to meet compliance requirements.

Additional Tools to Strengthen Security

Web Filtering

Email Filtering

Network Access Controls

Encryption

Vulnerability Scanners

Antivirus Software

Backup & Recovery Tools

Firewalls

Thank you for joining us today!

Any questions?

PNI HCM GovConPay Focus Matters

Join Us Next Month!

Open Enrollment: The Insider Ins & Outs of Seamless OE in isolved

Tuesday, August 12, 2025 at 1 pm

Scan to Register!