Using 2FA and biometrics for password reset.

How to secure and simplify your password reset process.
Passwords are Expensive

We live in a hyper-connected, technology oriented world where everyone can stay connected from practically anywhere, anytime. With all this connectivity, one might ask the question “How secure are we?” Every day, you log into multiple locations from a multitude of devices: Facebook, Gmail, PayPal, your brokerage account, your healthcare portal, and many more.

According to the NDSS Symposium, an average user maintains 25 distinct online accounts, but with only 6-7 passwords; 43-51% of users reuse their passwords.

80% of security breaches take place not through hacking or virus attacks, but through system infiltration facilitated by the use of a known password.

1.2 billion username and password combinations and over 500 million email addresses were amassed by hackers in one of the largest known collections of stolen credentials and confidential materials.

Industry studies show it can take at least 40 minutes for Help Desk personnel to manually reset a user password. Also, up to 50% of Help Desk tickets involve manual password resets.

Manual password resets may cause significant risks and costs to an organization’s bottom line, including:

- **Reduced Productivity**
  Business-wide slow downs often occur when password resets negatively impact user productivity with long wait times during business hours. This can be even worse outside of 9-5 operations, when help desk operations are typically either on call, or not staffed at all.

- **Reduced Customer Satisfaction**
  When customer passwords are locked, customer-facing service personnel are often unable to assist them. This can put Service Level Agreements at risk, and increases the potential of losing customers.

- **Phishing Security Risks**
  When customers reset their passwords manually, the potential exposure of critical user information increases the risk of hacker phishing.

- **Tracking Issues**
  Tracking manual password resets can be challenging and can cause audit and regulatory violations.

- **IT Resource Usage**
  On average, an IT Help Desk perform $125,000 worth of manual password resets per year (2,500 resets at $50 each). Often additional Help Desk resources need to be allocated, or worse, reallocated from other projects, which can be costly and time-consuming.

---

4. Reduce IBM i Help Desk Costs with Self Service Password Reset, 2015. seasoft.com – goo.gl/4cnD2k
Current Password Reset Approaches

Currently, many companies use Password Management (PM) tools to enable users to reset their own passwords. PM tools can also synchronize passwords for users across multiple systems, which allow users to access multiple applications with the same password.

Two Major Categories of Password Resets

- **Self-Service Password Reset (SSPR)**
  Typically performed by end users on demand.

- **Manual Password Reset**
  Usually performed by customer service or IT help desk as needed.

Because of its significant cost-savings and headcount-reducing benefits, SSPR is widely adopted. SSPR is usually treated as the first level of support, followed by the manual password reset process. It is worth noting that the Self-Service Password Reset (SSPR) functionality of PM tools does not reduce the number of passwords that a user has to remember, nor does it ease users’ pain associated with complicated password policies. This paper focuses on Self-Service Password Reset.
KEY FINDINGS
The following provides a summary of the most commonly used password reset approaches and their associated advantages and disadvantages.

Traditional Method
Usually initiated by a call into a help desk via a customer service line. Users call customer service to answer a list of pre-defined questions (knowledge-based). This is an expensive proposition when considering the overhead of the extra customer service staff needed. This only provides a “perception of security” as answers to some of the pre-defined questions can be found via social media or guessed by friends and relatives.

Automated Approach
There are three types of automated approaches for password reset:

1. **Online reset**
   - Convenience
   - Widely adopted
   - Answers to pre-defined questions can be easily guessed (friends, social media, etc.)
   - Answers to aged questions (10 year old phone number) can be easily forgotten

2. **Email reset**
   - Convenience
   - Widely adopted
   - Hacker access to email address/password possible

3. **Text message**
   - Convenience
   - Out-of-band authentication
   - Lack of security
   - Keycode complexity
   - Hacker/thief access to stolen/lost device

These methods aim to automate the password reset process, by either answering a list of pre-defined questions on a web browser, sending a temporary password to an email address, or a text message to a phone number. These approaches provide some level of convenience, but are almost entirely lacking in security.

Secure Automated Password Reset Approaches

**Devices/Tokens with One-Time Passwords (OTP)**
RSA tokens are an example for this category. A user carries an extra device that shows a string of numbers that change from time to time. This approach increases security somewhat, but it is expensive for the company. It adds another layer of infrastructure and is inconvenient for the users since they need to keep track of a single purpose device, then read and retype codes each time.

**Biometrics**
Using human traits as a password for authentication is clearly the winner in terms of convenience. You don’t forget your biometrics as they are always there. Whether it is your face, voice, fingerprints, iris, palm vein, etc., one always possesses them; they are unique to each individual.

**Multi-Modal Biometrics**
Using a single biometric fails to provide flexibility and adaptability for different use cases, such as voice authentication in a loud environment or a face recognition in a dark location. Also, by fusing multiple biometric traits, the level of security is greatly increased.

Table 2 illustrates an overall comparison of various password reset approaches. The highest level of security and the lowest cost are solutions using multi-modal biometrics.
CRITICAL ELEMENTS OF AN AUTHENTICATION SOLUTION

Biometrics are like your own personal password that cannot be forgotten, lost, or stolen. Users no longer need to remember the answers to their own password reset questions, nor do they need to carry a separate single purpose hardware token. They also do not need to re-type the complex, temporary password.

When evaluating biometric security solutions, your minimum criteria should include: two-factor authentication, multi-factor authentication, multi-modal biometrics, anonymous biometric storage, cloud-based matching, scalability, real-time performance, and versatility

Two-Factor Authentication
A combination of knowledge based information (something you know) and a physical device (something you have).

Multi-Factor Authentication
A combination of knowledge based information (something you know), a physical device (something you have), and biometrics (something you are).

Multi-Modal Biometrics
Using more than one biometric modality (i.e., face and voice) provides a substantially greater level of confidence for identity verification.

Cloud-Based Storage and Matching
While the use of biometrics greatly increases the level of confidence for identity verification, you must ensure that your captured biometric data is kept secure. Biometric images stored on mobile or desktop devices are subject to electronic theft. By storing your biometrics in a secure data center, the protection of your biometric information is greatly increased.

Anonymous Biometric Storage
Storing biometric data anonymously (i.e., separate from any user identifying information), renders any compromised information completely worthless to potential hackers.

Scalability and Performance
You need a biometric system that is ultra-scalable in order to provide real-time performance.

Versatility
The biometric solution needs to fit into any existing business processes.

IMAGEWARE’S GoVerifyID ENABLES AUTOMATED PASSWORD RESET

GoVerifyID enables you to add biometrics to your existing Self-Service Password Reset process.

For example, to reset their password, a user is prompted to speak a pre-recorded passphrase, such as “I am Jane Doe living in California,” and/or take a selfie.

With biometrics of their choice, the user’s identity is validated and their password reset.

Key benefits of this solution are:

Enhanced Security
Makes the password reset process your most secure internal IT process with multi-factor and out-of-band authentication.

Reduced IT Helpdesk Costs
By reducing the need for IT help desk agents to complete password resets, an organization can save up to 50% on help desk tickets.¹

Improved User Experience
Makes resetting a password literally as easy as speaking “My voice will reset my password.”

¹ Reduce IBM i Help Desk Costs with Self Service Password Reset, 2015. seasoft.com – goo.gl/4cnD2k
When it comes to resetting passwords, it is optimal to choose security solutions that provide the highest level of security, the best user experience, and are able to support your business processes. Biometric traits cannot easily be shared with others, which leads to information security and identity authentication management leaders to use them where data and system security is paramount. The challenges of using complex passwords and various kinds of tokens in user authentication, including mobile use cases, are driving interest in biometric authentication methods.

When multi-modal biometrics are combined with mobile and cloud technology, you can achieve the ultimate level of security, convenience, and usability for Self-Service Password Reset. ImageWare’s GoVerifyID provides this combination of features to best address the Self-Service Password Reset market.

By adding GoVerifyID to your password reset solution, you add out-of-band authentication along with multi-modal biometric identity verification on your mobile devices. This provides the ultimate level of security along with user convenience for the password reset process. The solution is a very secure scalable, simple to setup, and a real-time performance system.
About ImageWare

ImageWare Systems, Inc. provides end-to-end digital identity proofing, authentication and management solutions as a cloud SaaS and on-premises. The company's Digital Identity Platform provides customers and partners with access to its patented technology for ultra-scalable and anonymous biometrics using nearly any vendors’ biometrics. IWS solves the problem that is responsible for over 80% of corporate data breaches by replacing or strengthening passwords with your choice of biometrics and other multi-factor authentication methods providing the highest level of user assurance, security and user convenience. ImageWare Systems, Inc. is headquartered in San Diego California, with offices in Oregon, Canada, Mexico, and Japan. ImageWare and GoVerifyID are registered trademarks of ImageWare Systems, Inc. Other trademarks are owned by their respective vendors. Learn more at iwsinc.com.

Connect

@iwsinc .linkedin.com/company/imageware-systems-inc  facebook.com/imagewaresystems