



Password Theft

Poorly stored passwords, like those written down near computers, can be easily stolen.



Observation

A person can steal a password simply by watching someone type it in, often in public spaces.



Eavesdropping

Passwords can be captured by attackers as they move across a network, especially if the connection is not secure.



Brute Force

Hackers use automated software to systematically guess vast numbers of password combinations until the right one is found.



Leaked Passwords

Hackers use stolen passwords from breaches on one site to try accessing accounts on other systems.



Hash Cracking

Encrypted password hashes can be stolen and cracked, revealing the original password using specialised tools.



Common Password Attempts

Attackers try a few common passwords across many accounts in hopes of gaining access.



Guessing

Passwords can be manually guessed using familiar details like birthdates, names, or common words related to the user.



Keylogger Attacks

Attackers install keylogging malware to record keystrokes, capturing passwords as they are typed.



Social Engineering

Tricking individuals into providing their passwords through deceptive messages or coercive tactics.

Password Best Practices

What to Do

- Do** use passwords where necessary. We'll use other secure options (like fingerprint scans) wherever possible.
- Do** use Multi-Factor Authentication (MFA) for important accounts. It's an extra step that makes your login more secure.
- Do** choose long, strong passwords that are hard to guess—think of a phrase or a combination of random words.
- Do** use a password manager to store your passwords safely. It can also help you generate strong passwords.
- Do** check for "HTTPS" before entering passwords on any website to ensure it's secure.
- Do** protect accounts that need extra security, like admin and cloud accounts.
- Do** contact us if you suspect your password has been compromised, and change it immediately.

What to Avoid

- Don't** reuse the same password across work and personal accounts. Keep them unique to reduce risks.
- Don't** use obvious information like your name, birthdate, or pet's name in your password.
- Don't** share your passwords unless absolutely necessary. If you must share access, use the tools we provide instead.
- Don't** worry about changing your password regularly unless you think it's been compromised.
- Don't** write down passwords on sticky notes or leave them visible near your workspace.
- Don't** use common or simple passwords like "123456" or "password."

Advanced Safeguards & Handling Sensitive Data (1/4)

1. Additional Security for Sensitive Accounts

Multi-Factor Authentication (MFA): All accounts that access sensitive data or manage critical business functions (e.g., admin accounts, cloud services, HR systems etc) must use MFA as a standard. This ensures that even if a password is compromised, the attacker cannot access the account without the second layer of authentication.

Access Control Levels: Employees should only have access to the information and systems required for their work.

Use of Encrypted Channels: Always ensure data, especially login credentials and sensitive information, is transmitted via encrypted channels (e.g., HTTPS, VPN). Additionally, never send a username and password in one message. Use two formats for each section where possible (i.e. password sent via email, username sent via WhatsApp).

2. Secure Remote Work Practices

Remote Access: All remote access to Hunrosa's systems must be done through secure methods such as a **Virtual Private Network (VPN)** or trusted remote desktop solutions with end-to-end encryption.

Device Security: Employees working remotely should ensure their devices are password-protected, and company data must not be stored on personal devices.

Secure Storage: Sensitive data must not be stored on external drives or cloud services that are not authorised by Hunrosa. If such storage is necessary, it should be encrypted using strong encryption standards (e.g., AES-256).

Advanced Safeguards & Handling Sensitive Data (2/4)

3. Password Protection for Administrators

Stronger Password Requirements: Admin accounts must use passwords that are longer and stronger than standard user accounts. A minimum of **16 characters** with a mix of letters, numbers, and symbols are required.

Regular Password Audits: Password strength and usage audits for admin accounts will be undertaken regularly. This includes reviewing password expiration policies and ensuring that only necessary individuals have access to admin credentials.

No Shared Admin Accounts: Admin accounts must not be shared between employees. Each admin must have their own unique login to ensure accountability and traceability.

4. Handling Password Compromises

Immediate Reporting: If an employee suspects that their password has been compromised, they must report it to Hunrosa immediately and change their password.

Automated Alerts: Where possible, automated alerts will be implemented for failed login attempts, password changes, and other suspicious activity to prevent or contain breaches early.

5. Password Management and Expiration

Password Managers: Staff are to use password managers to securely store passwords. Password managers generate and store complex passwords and prevent reusing the same passwords across multiple accounts.

Password Expiration for Admins: Admins should change their passwords every 3 months or after any indication of a potential security breach.

Monitoring Password Sharing: Any shared password activity (if necessary) must be closely monitored, with logs maintained to review who accessed shared passwords and why.

6. Employee Training and Awareness

Regular Training: All employees to undergo annual security awareness training that includes password best practices, secure handling of sensitive data, and how to spot phishing attempts or other security risks.

Phishing Simulations: Random phishing simulations (without warning) will be undertaken to test employees' ability to spot suspicious emails, messages, and requests for sensitive information.

February 2025 Addendum

Operational Password Sharing Protocol (4/4)

7. Shared Password Instances

In specific operational cases where shared access is required for efficiency, the following accounts have been identified as requiring shared credentials:

info@ email account – Access shared between designated operational personnel.

Zoom account linked to info@ – Managed jointly by Hannah Bott, Kirstie Grantham and Danielle Tucker

Calendly and Eventbrite accounts – Managed jointly by Hannah Bott, Kirstie Grantham and Danielle Tucker

8. Secure Management of Shared Passwords

To maintain security while allowing shared access, the following measures must be implemented:

Storage in LastPass – All shared passwords must be stored securely in LastPass to ensure centralised, encrypted access.

Limited Access – Only the necessary individuals will have access to shared credentials. Any changes in team roles must be reported to update access permissions.

Regular Review – Passwords for shared accounts should be reviewed periodically to ensure they remain secure.

No External Sharing – These credentials must not be shared outside of designated personnel or stored in unapproved locations (e.g., email, spreadsheets).

9. Security Monitoring

Audit Logs – Where possible, account logs should be reviewed to track access and ensure security.

Multi-Factor Authentication (MFA) – Where supported, MFA should be enabled for shared accounts, with an appropriate method for verification between shared users.

Password Changes – Shared passwords should be updated if a team member no longer requires access or if a security concern arises.