RSI

PASSWORD ESSENTIALS

For Employees & IT Leaders

Password Essentials for EMPLOYEES

Employees and IT teams can work together on strong password practices as the frontline defense against phishing and other cyber attacks. By following these best practices, individuals and organizations can significantly improve their online security and reduce the risk of unauthorized access to their accounts.

Formulate a Strong Password Creation System:

- Use Strong, Complex Passwords: Create passwords that are at least 12 characters long and include a mix of uppercase and lowercase letters, numbers, and special symbols.
- Avoid Common Words and Phrases: Stay away from easily guessable words or phrases, such as "password," "123456," or "admin."
- Avoid Personally Identifiable Information (PII): Avoid birthdays, anniversaries or even nicknames in your passwords.
- Use Unique Passwords for Each Account: Never reuse passwords across multiple accounts. Each online service should have its unique password.
- Use Memorable Passphrases: Consider using passphrases, which are longer combinations of random words or phrases. They can be both strong and memorable.

1 Create a strong base password that will be used for each account password.

EXAMPLE:
7*dLeiK#

2 Add part of the account URL to the beginning and/or end of the base password.

FACEBOOK EXAMPLES
7*dLeiK#FB
FB7*dLeiK#
F7*dLeiK#B

3 Apply this password rule to all your current and future online accounts and you will have a strong, unique, and easy to remember password for each of them.

Source: Stickley on Security

Password Best Practices:

- Enable Multi-Factor Authentication (MFA): Whenever possible, enable MFA for your online accounts. This adds an extra layer of security by requiring something you know (password) and something you have (e.g., a mobile app or a physical token).
- Regularly Change Passwords: Changing passwords periodically can add an extra layer of security, especially for critical accounts.
- Beware of Phishing: Be cautious of phishing emails or fake websites that aim to steal your login credentials. Verify the source before entering your password.
- Secure Password Recovery: Ensure that password recovery options are secure, and only accessible to you. Avoid easily answerable security questions.
- Biometric Authentication: If your device supports it, use biometric authentication methods like fingerprint or facial recognition in addition to passwords.
- Secure Your Devices: Ensure the devices you use to access accounts are secure with passwords, PINs, or biometrics.
- Regular Updates: Keep your devices and software up to date to patch security vulnerabilities that attackers may exploit.
- Educate & Train: Educate yourself and your team about password best practices and security awareness. Regular training can prevent common pitfalls.
- Close Old Accounts: Close or delete accounts you no longer use, as they can become a potential security risk if left unattended.
- Backup Important Data: Regularly back up important data to prevent data loss in case of a security incident.

!! Apply these best practices to personal accounts as well. Cyber criminals are watching your personal accounts because they know that employees often use the same passwords for personal accounts as they do work accounts.

Password Essentials for IT LEADERS

In today's cyber threat climate, it has never been more important for IT leaders to arm their organization with the tools they need to protect organizational data. Password management is a critical component. It's no longer enough to encourage employees to update their online accounts with robust passwords. Employees need to be shown how, and IT needs to deploy additional measures as a backstop.

- Education & Training: Conduct regular security awareness training to educate employees about the importance of strong passwords, the risks of password reuse, and how to recognize phishing attempts.
- Implement Password Policies: Establish clear and enforceable password policies that define minimum complexity requirements, password length, and expiration intervals.
- Enable Multi-Factor Authentication (MFA): Require the use of MFA wherever possible, adding an extra layer of security beyond passwords.
- Regularly Update Passwords: Require employees to change their passwords regularly, especially for critical accounts. Consider using password expiration policies.
- Offer Password Management Tools: Provide employees with access to password management tools or recommend trusted third-party password managers to help them securely store and generate complex passwords.
- Block Common Passwords: Prohibit the use of commonly used and easily guessable passwords, such as "password123" or "qwerty."
- Implement Role-Based Access Control: Grant employees access only to the resources necessary for their roles to limit the potential impact of compromised accounts.
- Password Recovery Procedures: Establish secure password recovery and reset procedures to prevent unauthorized access to accounts through social engineering.
- Implement Account Lockouts: Automatically lock accounts after a specified number of failed login attempts to thwart brute-force attacks.
- Regular Security Audits: Conduct periodic security audits to identify weak passwords, inactive accounts, and compliance with password policies.
- Monitor for Breaches: Implement monitoring systems to detect and respond to suspicious login attempts or unusual account activity.
- Review Third-Party Access: Regularly review and revoke access for third-party applications or services connected to employee accounts to prevent unauthorized access.
- Password Storage and Encryption: Ensure that stored passwords are encrypted and employ secure hashing algorithms.
- Regular Updates & Patching: Keep all systems and software up to date to address known vulnerabilities that could be exploited to steal passwords.
- Incident Response Plan: Develop an incident response plan in case your accounts are compromised. Know what steps to take to mitigate the impact.

RSI, consults, architects, implements and supports complete IT and cybersecurity solutions.

About RSI: Since 1982, RSI has provided innovative technology solutions, advanced professional services and fully automated solutions for effective business workflow. With RSI, clients realize that relationships matter, and our quality is embedded into our culture. Through our proven Assess-Remediate-Maintain process, RSI helps clients manage complexity and drive a return on your IT investment. We serve the enterprise with proactive cyber security solutions, custom software development for business process improvement, and advanced IT operations to create greater efficiencies. rsitex.com