fasthosts ProActive

Oops-proofing your security

Password safety

Welcome to the second instalment of our “Avoiding Human Error” blog series. If you’re new to the series, we tackle some of the most common human errors that lead to security breaches and provide you with actionable tips to safeguard your business. Today, we’re focusing on the importance of creating and managing strong passwords.

Why strong passwords matter

Passwords are often the first line of defence against unauthorised access to your accounts and sensitive information. Weak or compromised passwords can easily be exploited by attackers, leading to data breaches, financial loss, and other serious consequences.

How to create a strong password

Creating a strong password doesn’t have to be difficult. Here are some key tips to follow:

1. Length – Aim for at least 12 characters. The longer the password, the harder it is to crack
2. Complexity – Use a mix of upper and lower case letters, numbers, and special characters
3. Avoid common words and phrases – Steer clear of easily guessable words or sequences, like the classic “password123” or your pet’s name
4. Randomness – The more random, the better. Consider using a passphrase made up of unrelated words

Tools to help create and manage passwords

To simplify the process of creating and managing passwords, consider these tools:

- Password managers – These can generate and store complex passwords for you. Examples include LastPass, 1Password, and Dashlane
- Two-factor authentication – Adding an extra layer of security makes sure that, even if a password is compromised, an additional step is required to gain access

Educate your team on password best practices

Making sure your team understands and implements password best practices is crucial. Here’s how to educate them effectively:

- Regular training – Conduct regular cybersecurity training sessions focusing on password management.
- Policy enforcement – Establish and enforce clear policies regarding password creation and management.
- Simulations and drills – Regularly test your employees with password security drills to keep them alert and aware.

Avoiding common password mistakes

Even with the best practices, mistakes can happen. Here's what to avoid:

Reusing passwords – Never use the same password for multiple accounts. If one account is compromised, others will be at risk.
Sharing passwords – Never share your passwords with anyone. If you must share access, use secure methods, like a password manager's sharing feature. This allows you to securely share passwords with others by encrypting them and controlling access permissions.
Ignoring security alerts – Pay attention to security alerts from your accounts and change your passwords if you suspect any suspicious activity.

What to do if your password is compromised

If you suspect that your password has been compromised, act quickly:

Change the password immediately – For the affected account and any other accounts that used the same password
Enable two-factor authentication – If it's not already in use, set it up
Monitor account activity – Keep an eye on your accounts for any unusual activity
Report the incident – Inform your IT department or security team so they can investigate and take necessary actions

Strong passwords are a cornerstone of robust cybersecurity. By implementing these practices, you can significantly reduce the risk of unauthorised access and protect your sensitive information.

Stay tuned for the next post in our "Avoiding Human Error" series, where we'll cover more essential tips to keep your data safe and secure.

If you have any questions about security, or think your infrastructure could benefit from a Managed Service Provider like ProActive, get in touch. You can call us on 0333 111 2000 or book a meeting at a time that suits you.