The information Commissioner's Office

Password storage – why it's not as simple as 123…

Posted on May 14, 2014by icocomms

Sadly, the most commonly used passwords continue to be '123456' and 'password'. While individuals have a clear role to play in using sensible passwords and not repeating their use across all websites, as an organisation there are still steps you should be taking to keep people's information secure.

As a first step, you should make sure that service users are able to use passwords that include a combination of numbers, symbols and lower and upper case letters, to access your website or service. By adopting this approach your users can create passwords which will take longer for hackers to crack, providing your organisation with more time to identify an attack and take action to stop it.

However, choosing a secure password and keeping it secret is the limit of what a user can do to protect themselves. It is then up to the data controller to protect the user's data.

The secure storage of passwords is an important backstop to reducing the damage an otherwise successful attack on your IT systems can bring. Many recent IT security breaches would still have occurred regardless of the methods used to store people's passwords. However, storing passwords in a secure manner limits the potential for further damage as the attacker is still unable to access the passwords in a useable form.

This is where two techniques known as hashing and salting can be extremely effective. While they may sound like terms coined in your local greasy spoon café, they are important techniques for keeping individuals' password details secure that your organisation should be using.

In short, hashing is a cryptographic technique which can transform readable text, like a password, into a different set of data of fixed length. Salting is a further technique that adds some random data to the mix.

Together they can make a password virtually incomprehensible to an attacker and their use is considered best practice across the IT security industry.

Further guidance on the use of hashing and salting can be found in the password storage section of our IT security report, (see below) however the key points to remember are that:

- Storing passwords in plaintext is not appropriate.
- You need to salt and hash your users' passwords, and store the hashed values only and not the passwords.
- The hashing method used needs to be up-to-date to make it difficult for an attacker to guess passwords.

Finally, you also need to consider what actions you will take if the worst should happen and your users' access credentials are breached. How will you communicate this to your users and if you take the decision to revoke all passwords, how will you be sure that the user attempting to sign-in and reset the password is the owner of the account? Don't forget that the attackers could also have a list of your users' email addresses and use these for malicious purposes. You must prepare for this eventuality by having a secure process in place to make sure the people you are allowing to access your accounts are the real deal.

Our report includes useful information and advice on the measures organisations should have in place to keep passwords secure, including further details about the ins and outs of hashing and salting. Review your existing processes against the report in order to make sure you're not allowing your customers to become an easy target.

Password hashing – good practice summary:

- Don't store passwords in plain text, nor in decryptable form.
- Use a hash function. Only store the hashed values.
- The hash function should have appropriate strength to make offline brute-force attacks extremely impractical.
- Use salting to make offline brute-force attacks less effective.
- Periodically review the strength of the hash function and keep up to date with advances in computing power. The best way of achieving this is to use a password hashing scheme with a configurable work factor.
- Use a combination of password strength requirements and user-education to ensure that attackers can't simply guess common passwords.
- Have a plan of action in case of a password breach. This should include how to reset users' passwords in bulk and how to notify them of what has happened and what they need to do about it.