

Passwords

- Does your company have a password policy?
- Do you have a password to access your computer and separate passwords for different applications?
- Is your password at least 8 alphanumeric and special characters?
- Do all of your computer users have their own machine (i.e. no hot desks)?
- Do all staff have separate logins?
- Are passwords changed regularly?

If you answered no to any of the above then your business is at risk.

Description

Consider the implications if your passwords were cracked and criminals gained access to your accounts. Money could be stolen, personal and sensitive emails could be read and your business and personal life could be heavily disrupted.

- + A password with 6 letters all the same case has 308 million possible combinations. Whilst this may seem like a lot, hackers with readily available software can crack this in less than 3 minutes
- + A password with 6 both upper and lower case letters now has 19 billion possible combinations. Increasing the password to 8 letters makes 53 trillion combinations
- + A password 8 characters long incorporating upper and lower case letters, a number and a special character will result in 6,095 trillion possible combinations

Improving passwords is a cheap, easy and effective way of boosting a business' security. They are not the complete solution and a dedicated hacker with the right tools will be able to get past them, but they will slow an intruder down and act as a deterrent.



CASE STUDY

Telecoms &

Communications

Business, Manchester

“As a business we never really considered passwords and account management to be that important. We knew that we needed them but didn’t understand their significance as the first line of defence against hackers and criminals or that an attack could come from internal sources.”

The company is a mobile communications company selling contracts to business users. They were recently the victim of internal data theft that could have cost the business heavily.

The internal database housed all their client details, length of their air-time contracts, their payment details and when their contracts were up for renewal. Every member of staff had access to the database.

A member of staff who had recently left the company had used his account password to login and steal the client database, with the intention of using the information to approach existing customers with improved deals, and steal their custom.

The business did have a procedure in place so that anyone submitting their notice would be immediately escorted from the site to stop the potential for stealing data, but no protocols were in place to stop it happening remotely after they had left the site. If one of their loyal customers had not contacted the business to warn them of an approach, the company could have been severely damaged.

What the company should have done was ensure that they had a password policy in place which outlined the duties of the employee to ensure their password followed all of the usual security criteria. It should also ensure that as soon as an employee left, their account was deleted. The policy would also have ensured all other members of staff change their passwords on a regular basis.

Solutions

- + Your password should be at least 8 characters long ideally, 16 is best. Utilise a combination of different cases, numbers and special characters such as !@#\$%^&*;,”
- + Use a phrase that is going to be difficult for anyone to guess
- + Use different passwords for different accounts. At least if one of your passwords is lost or cracked then your other accounts will remain safe
- + Change your password at least every 30 days so that any undetected hackers can no longer use it
- + Do not reuse more than 50% of characters in a new password
- + Don't use sequences or repeated characters like ZZZZZZ or 123456
- + Don't use your login details or any part of your name as these will likely be the first things attempted by a hacker
- + Never write your password down, if you feel you may forget it, then write a prompt, cryptic clue, or use patterns of keys on your keyboard
- + Never send a password through email. Emails are not considered a secure form of communication
- + Never reveal your password over the telephone
- + Never hint at the format of your password or the subject
- + Never reveal or hint at your password on a form on the internet
- + Never ask to see someone else's password
- + Never use the "Remember My Password" feature of websites such as Microsoft Internet Explorer, your email program, or any other program
- + If anyone asks for your password, report them to your IT manager
- + Make use of the password checker on Microsoft's website – <http://www.microsoft.com/protect/yourself/password/checker.mspix>
- + Ensure you have a password policy. Go to www.bcrc-uk.org for a sample policy

Useful Websites

<http://www.ktn.qinetiq-tim.net/>
<http://www.berr.gov.uk/whatwedo/sectors/infosec>
<http://www.bcrc-uk.org>
<http://www.businesslink.gov.uk>
<http://www.getsafeonline.org/>
<http://www.sophos.com/security>
<http://zdnet.co.uk/toolkits/securitythreats>
<http://www.microsoft.com/protect/yourself/password/checker.mspix>

