VIRUS ALERT
Your machine is infected with Cryptolocker.
Please pay £2000 for the decryption key and
the return of your files

Password Essentials
Network ROI are committed to keeping you safe online.
Use this guide to help protect your valuable business data.
Why You Need a Strong Password

Whether you’re logging into Office 365 at work or signing into Amazon, Netflix or Facebook, passwords are an essential part of daily life.

Passwords exist to protect valuable information stored on personal and company devices. Passwords also protect the computer systems of companies you do business with from the attention of organised criminal gangs who wish to profit from your valuable data.

Recently, data such as user credentials, bank details, personal addresses and passwords have become a precious commodity to online fraudsters looking to profit from the trusting nature of honest, hard working people.

The number of logins we now have to deal with every day also means we’re more likely to re-use the same password for multiple sites; a dangerous tactic that potentially lets criminals penetrate multiple sources of information at once.

Recent hacking incidents aimed at high-profile companies such as Sony, Apple and Talk Talk have highlighted a very real need for businesses to take online security much more seriously. The companies mentioned, as well as many small, less well-known enterprises, are counting the cost in lost profits, reputational damage and loss of consumer trust.
Three Common Tactics Used by Hackers

Brute Force Attack
A Brute force attack is a method of breaking into a computer network based on a trial and error approach which attempts to guess every character of your password using hundreds of thousands or even millions of attempts. Brute force attacks are time-consuming and easily preventable with account lockout policies, similar to the ones implemented by Network ROI.

Dictionary Attack
A dictionary attack is a method of breaking into a computer network based on trial and error but unlike the brute force attack, the dictionary attack uses a list of common words used in passwords. Every time a dictionary attack is successful, it adds the cracked password to its own database.

Dictionary attacks guess passwords much faster than brute force because they are targeting a smaller amount of commonly used passwords. Account lockout policies provide a degree of protection against these types of attack, but won’t stop them all.

Password Spraying
Password Spraying is a method of breaking into a computer network based on guessing the username with a commonly used password. Password spraying works against lockout policies by limiting the number of attempts to break into the network against any single account. Password spraying usually targets thousands of machines at once.

Other common hacking techniques

- social engineering
- manual password guessing, using personal information ‘cribs’ such as name, date of birth, or pet names
- intercepting passwords as they are transmitted over a network
- ‘shoulder surfing’, observing someone typing in their password at their desk
- installing a keylogger to intercept passwords when they are entered into a device
- searching an enterprise’s IT infrastructure for electronically stored password information
- finding passwords which have been stored insecurely, such as handwritten on paper and hidden close to a device
- compromising databases containing large numbers of user passwords, then using this information to attack other systems where users have re-used these passwords.
Password Tips

Always change default passwords

Cracking a default password is the first thing a hacker will try when looking to exploit your network. **Important - Always change the initial password issued by Network ROI on first use.**

Sharing passwords

Never allow login or account sharing between users. Doing so negates the benefit of authenticating a specific user, making it extremely difficult to audit and monitor the action of users.

Never use the same password for multiple sites or accounts. If the password for one site or account becomes compromised all information will be under threat. This advice applies to both work and personal accounts.

Don’t change a strong password unless you think someone else knows it

Many security policies recommend you change your password every 30, 60 or 90 days. The National Cyber Security Council (NCSC) now suggests you don’t change a strong password regularly. Read [this article](#) for more information on this new best practice.

**Only change a good password if you think someone else knows it. If you do have to change the password, make the change significant - i.e. don't just add a number or symbol to the end.**

How strong is my password?

Safely test the strength of your password here - [https://www.my1login.com/resources/password-strength-test/](https://www.my1login.com/resources/password-strength-test/)
Password Do’s & Don’ts

Do

• Choose something that you can easily remember without writing down.
• Choose something that you can type quickly, reducing the chance of someone stealing your password by looking over your shoulder
• We recommend using a minimum of 10 and a maximum of 16 characters, which must be a mixture of upper case and lower case letters, numbers and symbols
• Use between two and four short, random words with spaces or symbols that join them together
• Use a good password generator software if you find the tips above tricky
• Use the first letter of each word from a favourite poem or song

Don’t

• Don’t use your name, company name or something personal to you that can be found on social media such as birthday, dog name, child name etc.
• Don’t use the same password for multiple sites or between home and work accounts
• Don’t base your password on something located close to you such as mouse, monitor, keyboard etc.
• Never use the word password in any form. e.g. ‘Pa$$w0rd’ or ‘pa55word’
• Don’t use a single word found in the English dictionary, or a foreign one for that matter
• Don’t use a simple keyboard sequence such as ‘qwerty’, ‘zxcvbnm’ or ‘abcdefg’
• Don’t use the name of your favourite sports team, actor or musician, especially if that information can be easily found on social media
• Never use a password based on your name, account name, username or email address
• Don’t simply double up on a word. e.g. “bookbook”
• Don’t reverse a word. e.g. ‘koob’
• Don’t rely on adding numbers to replace letters in common words such as ‘5pac3man’ or ‘m0n1tor’
• Don’t change a strong password regularly - test your password here
Password Resources

There are lots of great resources available to help you manage passwords for both business and personal logins. Here are some examples of commonly used password generators and password management tools.

- **Diceware Passwords**
  Password Management

- **xkcd Password Generator**
  Password Management software.

- **Lastpass**
  Password Management software.

- **KeePass**
  Open-source password management software.

- **Password strength meter**
  Test the strength of your password.

- **Password Guidance: Simplifying your approach**
  Official Government advice for creating simple and effective passwords

Password Examples

Here are some examples of both good and bad passwords. The trick is to find something that is both memorable, but difficult for a machine to guess. The example at the bottom of the list below will be extremely difficult for a machine to decipher, but also difficult for you to memorise.

Also, never use the actual examples shown in any password resource as there is a good possibility they have been added to a criminal database somewhere.

**Bad**
- Pa55w0rd
- Pa$$w0rd
- qwertyuiop
- Liverp00lFC
- 1234567890

**Good**
- Rose-Lion-Ring!
- 1Rose2Lion5Ring!
- 1R0se2L10n5R1ng!
- 1r0Se2L10n5r1nG!