

[Press Releases](#)[Case Studies](#)[Microblog](#)[Blog](#)

Password security

Over the past few months, I must have had to remember hundreds of passwords, thinking of all the projects we have been working on. That is on top of all of those other passwords I need outside of work for my own website, to network socially and to check how much money I have not got in the bank. This ever-growing complexity, and demand on my increasingly limited memory, has left me mulling over the importance of password security.

While writing this post, I've read quite a few articles about password security. Many of them open with one of two pitches. The first is that passwords are annoying. The second is that you need to be *really* paranoid about your security online. Now the first is true and the second probably doesn't hurt, but both are distractions from what a password should be. A good password should be like having a good lock on a door. It's the difference between a good, solid five lever deadbolt lock and something that can be opened with a credit card.

Passwords are a good, cheap form of security. Just as you can fit a door with security systems from the next Tom Cruise Mission Impossible blockbuster, you can, in principle, fit a website with a variety of gadgets for authentication, like the card readers available from some banks. In most cases, the cost of the extra security will outweigh the benefit if the passwords used are strong.

While passwords are used in lots of places, I'm specifically interested in protecting content management, ecommerce and other systems and services that make up websites. These passwords may be used to access your site's CMS or might be protecting services hosted elsewhere like Google Analytics or Twitter that you use for your business.

Password Cracking

If a hacker can find where to log in to a site's administration system, they can attempt to break into it by guessing or obtaining a password. There are two basic ways they can do this: guessing and social engineering.

If a password is really bad; say a password of "password", "12345" or "qwerty"; a hacker may be able to guess it and try it manually. If they are a little more determined, they may resort to using software to try a list of commonly used passwords. An automated software attack might try a dozen passwords or it might try many thousands of possible combinations.

Social engineering relies on some of the skills a con artist uses to take money from the unwary and a variety of investigative skills. They persuade you to give up your password, they work it out from information they can find out about you, they go through your rubbish for scraps of paper you've thrown out and they gain access to where you've got the password written down on a post-it note by a variety of ruses.

Bad Passwords

There are a range of things you can do to make it hard to guess or break passwords by an automated attack.

To make it hard for them to crack or guess using easy to discover information about you, don't use:

- Dictionary words
- Names or other proper nouns
- Foreign words

Search

via your interest

via keyword or phrase

Talk to us

Name

How would you like to be contacted?

Email Phone

Email Address

Avoid personal information like:

- Phone numbers
- Birthdays
- Car registration
- Postcodes
- Children, spouses or other relatives names

Don't use business information such as:

- Business names
- Business address
- Web site address or name
- Product name

Don't try to make a bad password good by, for example, using a backwards version of a bad password, or obvious substitutions like 3 for E or K for C.

Good Passwords

Good passwords are usually longer. They should be at least 6 characters long. They should include a variety of characters not just A to Z. Good passwords should include special characters (like @, + and #) and numbers. Many systems will let you use uppercase as well as lowercase letters or spaces. Some systems may allow Alt characters to be used. Specific systems may have specific security features you need to be aware of.

Keeping it Safe

Once you've got a good password you need to keep it safe.

Don't give out passwords, especially not to requests by e-mail or phone. If a researcher offers you chocolate for your password when you get off the bus, do tell them a fake one. You shouldn't be denied chocolate in the name of security.

Don't share passwords with other people. If you can have separate accounts, make sure everyone has their own account. Shut accounts for users who have left. Not just because someone who has left may not care as much about your security anymore but because an unused account is a tempting target for an attacker.

Don't use the same password on multiple systems. Especially don't use the same password for personal and work systems. That way if one of them is breached you are only worrying about problems at work or home, not both at once.

If you need to keep a record of an important password, which cannot be recovered or automatically reset, put it somewhere secure. Ideally put it in a sealed envelope with a signature over the seal and put it in a safe or a secure, locked container. When you change a password, destroy any record of it by shredding it.

Avoid putting them on post-it notes or under your keyboard. This is the equivalent of putting a key under the plant pot by your front door.

It's also a good idea to change your passwords every few months.

Passwords for New Users

Many systems require an administrator to create accounts for new users and allow them to set up the user's starting password. Avoid using weak passwords when giving them out to new users as a shockingly large number of them will never change them, especially if they are easy to remember. Also don't use the same one for several users.

Going a bit Further

There are a wide variety of other measures you can consider in addition to using good passwords which won't cost you the earth. We are very happy to work with our clients to

discuss ways in which they can help improve security.

 [Subscribe to blog comments RSS feed](#)

Site Links

[Sitemap](#)
[Terms & Conditions](#)
[Accessibility Statement](#)
[Privacy Policy](#)

RSS Feeds

[Announcements](#)
[Blog RSS Feed](#)
[Twitter Feed](#)

Site Validation

[W3C XHTML 1.0](#)
[W3C CSS 2.0](#)
[W3C Accessibility WAI-AA](#)

Accreditation

[ISO 27001](#)
[ISO 9001](#)
[Institute of IT Training](#)
[PRINCE2](#)
[Buying Solutions](#)

Partners


immediacy
MEDIA&MARKET


RedDot
The Open Text
Web Solutions Group