KEEP YOUR VALUABLES UNDER LOCK AND KEY

Business & Management shares advice on how to protect valuable company data and hardware with better password management

When the world's worst passwords are published annually, there is a shared air of amusement that 123456 is still the most popular login. But for businesses, good passwords are integral to protecting confidentiality and reputation. In October, it was revealed that the Yahoo hacking had extended to every user account – indicating that, with increased computing power, hackers can run 'brute force' attacks by checking random combinations at speed. No one wants their business exposed, least of all because half the workforce is using a dud password – and because in May 2018, the General Data Protection Regulation will introduce much larger fines for security breaches. Here are our top tips for ditching bad password habits.

01

KNOW YOUR VULNERABILITIES

The first step to better password management is to assess how they can be compromised. The most basic security should not be taken for granted.

Default passwords, according to the National Cyber Security Centre (NCSC) established by GCHQ, should be changed at the earliest opportunity. Be alert to your workforce sharing passwords for their convenience. Human error and fraud are among the top reasons systems can be compromised. If someone is aiming to defraud or access important files, obtaining this level of trust is likely to be part of the hacking arsenal.

Indeed, the NCSC identifies techniques employed by individuals to gain passwords. Moreover, information on using these techniques successfully is easily found online. Methods include: social engineering/phishing; manual guessing; interception over a network; looking over someone's shoulder; installation of keystroke logging software; searching IT infrastructure for stored passwords; looking for handwritten notes; or compromise of a database.

Some of these take advantage of individuals experiencing password overload. So many websites require login IDs, people create unsecure strategies to help remember or store them. Mark Taylor, a technical manager in ICAEW's IT Faculty, says: "Never use the same password between systems or services.

"If a hacker gets your password from one place they will try to use the same one at a second service."

02

AIM FOR STRENGTH

Dialog boxes often pop up during password creation to tell us how safe our password might be according to that particular organisation. But what does a truly strong password look like? Taylor is an advocate of a passphrase as an alternative to the traditional password. This follows the principle that something longer may work better than something seemingly complex in the face of a brute force attack.

Making a complex password with random capital and lower case letters, symbols and numerals feels as though it must be secure; as a password it's certainly unmemorable and at risk (see 1 above). A passphrase, however, could consist of four random words that are easily memorable. It does not seem possible that this will be harder for hackers to break – but it is. The US computer scientist and blogger known as Crambler tested a series of long, simple password combinations against complex ones, using the sites How secure is my password and Passfault Analyzer.

In his analysis, an eight-character common word, eight random characters, or eight random characters with numbers were all deemed useless. Those with added symbols were deemed risky. Of the random selection J5bZ>9p! he says: "Sites call passwords like these strong, but in reality many of them could be hacked in under a day by a determined hacker."

By contrast, the passphrase 'I own 2 dogs and 1 cat' was deemed to be secure forever: the shortest time predicted to crack it was given as a sextillion years. Adding further complexity, such as a mixture of numerals and words in the combination, and even a grammatical error – 'I own two dogs, and 1 cats' – might lengthen the odds again.

Taylor also advises against using a simple word as a password and thinking it secure just by substituting characters, ie, a number four for a letter 'A', or a zero for an 'O'. "This makes it easy for a computer trying to guess at a rate of 1,000 guesses per second." He says four common random words "could take a computer up to 550 years to crack searching at the same rate".

SECURITY HOLE:
THE 10 MOST COMMON PASSWORDS

The list, compiled by security research firm Keeper Security, analysed more than 10 million passwords. A whopping 17% of computer users were locking their accounts with the top entry, 123456, with five more of the top 10 using a variation on this pattern.

1. 123456
2. 123456789
3. Qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. Password
9. 123123
10. 987654321

03

CONSIDER TWO-FACTOR AUTHENTICATION

Another method of security is two-factor authentication (2FA). One basic method of 2FA is to be sent an SMS when your computer is accessed or logging into an account from a new location (a method already employed by banks and webmail providers). Researching 2FA that best suits your business needs and budget may take time, but there are many security companies offering quotes on their software. You could also make it company policy for workers to switch on the 2FA services embedded within smartphones that are used for company purposes (see 6 overleaf).

Biometric scanners using eye or fingerprint verification can provide additional security in two ways; not only could a remote hacker not use your fingerprint or eye, even if your password is discovered, Taylor says it is unlikely criminals will have access to the application or device required to work with the extra set of codes or reference points.

04

CONSIDER A PASSWORD MANAGER

Taylor and the NCSC are in favour of using password managers. These allow individuals to use one master password and, within the system, store encrypted versions of other passwords. Password managers can be run with user-generated passwords or create them for you – those generated by password managers are thought stronger than anything someone could create at random themselves.

Password managers also help to eliminate one of the most serious security holes – reducing the need to write a password down. Some password managers work in conjunction with 2FA, such as smartphone fingerprint scanners. There are many password managers on the market, including Dashlane; LastPass; Sticky Password Premium; LogMeOnce; Roboform; Zoho Vault; Password Boss; Keeper; Agile Bits; and True Key.

However, Taylor has this warning regarding password managers: “They are very helpful but they’re not entirely infallible – there have been instances of breaches detected by security researchers where it has been possible to gain complete access to accounts set up in password vaults.”

05

ENCRYPTION OR HASHING?

Password managers may offer the simplest way to encrypt data, but what does this mean? The following passage from NCSC might strike fear into the hearts of business managers: “Produce hashed representations of passwords using a unique salt for each account. Store passwords in a hashed format, producing a cryptographic function capable of multiple iterations.” It’s bewildering stuff for anyone with only a day-to-day working knowledge of computers.

The point of encryption is to ensure that no password you might have on a machine is stored as plain text, thus reducing the likelihood of a successful brute force attack on files. Taylor advises that encryption is vital for anyone whose business relies on the cloud. But the NCSC description above also mentions hashing. Simply put, the difference between encryption and hashing is that an encrypted string of unreadable characters can technically be reversed (or decrypted) while a hash is a “one-way” code where a salt (an extra string of long randomised code) is added. One advantage of hashing with a salt is that it makes it much harder for hackers to hold functioning

GILLIAN BLEASE/IKON

databases of pre-computed hashes (so-called hash files or rainbow files, which help them identify commonly used passwords) because it would make storage of the large file required more difficult and ensure a database search took much longer to carry out.

The NCSC advises that any password protection system uses "public standards, such as PBKDF2, which use multiple iterated hashes". The algorithm SHA-2 is widely considered the strongest level, with SHA-256 (producing a 32-byte hash value) viewed as crucial where the highest protections are required.

Businesses with no in-house IT security should enlist someone with appropriate credentials to do the work, rather than attempt DIY protection in a bid to save money.

06
ESTABLISH A COMPANY POLICY

To really beef up password management, senior management needs to be pro-active with the entire workforce, and do as the NCSC suggests – either implement a corporate password policy or regularly review and revise an existing one.

Businesses could first employ the principle of least privilege. Who truly needs access to the most precious information? It may be fewer people than at present. Decide which parts of the organisation's data need password protecting and to what level. The more complex the business, the more parts may need protecting, and with access granted to different groups of people depending on the individual's role and level of seniority. Standard users should not be granted administrator privileges, advises the NCSC. Administrator-level accounts could potentially override a system lockout, and are therefore deemed most worthy of hacking.

Those who have genuine administrator level access, as well as remote users of systems, should be prioritised when it comes to grading levels of protection, it adds. This could well be an important area of distinction when it comes to costing your security add-ons. Also determine who would most benefit from adding 2FA to system security.

Once the system is implemented, what will your protocol be for dealing with an attempted breach? Who will be responsible for administering the new policy and reviewing it at regular intervals? This person, or group of people, will need to understand the principles behind the security measures, ie, having some knowledge of the limitations of machine-generated passwords, and the likely effects of implementing measures, such as system account lock-outs to help protect a system.

For example, should a business decide that locking is worthwhile (for example, after a set number of failed attempts at logging in), if this has been attempted across the whole company, a denial of service will have been inadvertently created.

Another method to consider might be CAPTCHA, which asks users to click on specific pictures in a grid of images to prove they are not a robot, and blacklisting, which prevents people from selecting certain weak passwords within the business.

07
EDUCATE THE WORKFORCE

No policy will have any positive impact on your business if it is not implemented in conjunction with a training programme.

The workforce must learn both how to spot suspicious activity within password-protected systems, and also how to create effective passwords. Regular brush-up sessions can remind people of the limitations of passwords created by humans and, if you use password managers, hold best practice sessions. The NCSC also warns of the danger of relying too heavily on password strength meters to give assurance that a password is safe enough.

It adds: "Tell users that work passwords protect important assets; they should never re-use passwords between work and home." ●

DON'T MISS...
PRACTICAL PASSWORD POLICIES

8 February 2018 12:30
The Business & Management Faculty is holding a special session on password management as part of its regular lunchtime learning series. IT Faculty technical manager Mark Taylor will be guiding participants on the adoption of effective and efficient password policies for business.

Sign up for the webinar at icaew.com/lunchfeb

FURTHER RESOURCES

ICAEW cyber security resources
icaew.com/cyber

ICAEW IT Faculty
Webinar on best practice for password management.
Find the recording at:
tinyurl.com/BAM-PW-webinar

GCHQ's National Cyber Security Centre has also issued guidance:
tinyurl.com/BAM-NCSC-PWs

Information Commissioner's Office (ICO)
ICO.org.uk

General Data Protection Regulation – an overview from ICO
tinyurl.com/BAM-ICO-GDPR