Manufacturers will be banned from having weak, easily guessable default passwords

FIRST LINE OF DEFENCE

Alan Stephenson-Brown *reveals the true cost of a weak password and shares best practices to protect businesses*

New laws that came into force as recently as 29 April this year – as part of the Product Security and Telecommunications Infrastructure (PSTI) regime – are a welcome move that should significantly improve the UK's resilience from ongoing cyber attacks. Going forward, manufacturers of all internet-connected devices must implement minimum security standards. This will mean a clampdown on some bad digital habits that too many of us have become guilty of, but which have potentially devastating consequences for businesses.

The laws are coming into force as part of the PSTI regime, which has been designed to improve the UK's resilience from cyber attacks and ensure malign interference does not impact the wider UK and global economy. Manufacturers will be legally required to protect consumers from hackers and cyber criminals from accessing devices with internet or network connectivity – from smartphones to games consoles and connected fridges – as the UK becomes the first country in the world to introduce these laws. Under the new regime, manufacturers will be banned from having weak, easily guessable default passwords like 'admin' or '12345' and if there is a common password the user will be promoted to change it on start-up. The move marks a significant step towards boosting the UK's resilience towards cyber crime, as recent figures show 99 percent of UK adults own at least one smart device and UK households own an average of nine connected devices. The new regime will also help give customers confidence in buying and using products, which will in turn help grow businesses and the economy.

All this is intended to increase consumer confidence in the security of the products they buy and use, delivering on one of the government's five priorities to grow the economy. The new laws are part of the government's £2.6-billion National Cyber Strategy to protect and promote the UK online. If successful, the move will help prevent threats such as the Mirai attack in 2016, which saw 300,000 smart products compromised due to weak security features and used to attack major internet platforms and services. Since that incident, which left much of the US East Coast without internet, similar attacks have occurred on UK banks including Lloyds and RBS leading to massive disruption to customers.

Passwords play a crucial role in maintaining the integrity of corporate assets, yet in 2022, more than 24-billion passwords were exposed by hackers and around 80 percent of confirmed breaches are related to stolen, weak or reused passwords. Clearly, robust password policies are critical for ensuring the security of digital assets and accounts. Not only do they make it more difficult for hackers to access accounts, systems and sensitive information, as cyber threats evolve it allows organisations to adapt and respond to new challenges effectively. To fully understand the benefits of such policies, it's helpful to look at the consequences of using weak passwords.

Studies have found the most commonly used passwords in the UK last year were '123456' and 'password', which will now be disallowed thanks to the new legislation. But what's so bad about them? Weak passwords represent a significant security risk, exposing individuals and organisations to various threats, including unauthorised access, data breaches, identity theft, and loss of trust and reputation. Often short or easy to guess, they can be cracked in minutes using methods like credential stuffing. One survey found that 30 percent of respondents – all IT professionals – had experienced a data breach because of a weak password and an additional 23 percent were unsure whether they were involved in a data breach.

Because weak passwords can be easily guessed or cracked by automated tools, they make it easier for attackers to perform account takeover attacks and access to a user's account and misuse it for malicious purposes, such as stealing sensitive information or spreading malware. 560,000 new pieces of malware are detected daily and the first half of 2022 alone saw 236.7-million ransomware attacks globally, with an average cost of $4.54-million per incident. There has been an alarming increase in malware infections over the last decade, a trend set to continue, with the cost of cyber crime predicted to hit $8-trillion in 2023.

Additionally, weak passwords increase the risk of identity theft, where attackers impersonate individuals to access their financial accounts, make transactions or fraudulently apply for loans *etc*.

Approximately 1 in 10 Europeans claim to have recently experienced online identity theft (European Commission) and between $24-million and $55-million is lost annually to card ID theft in the UK (UK Finance). Lesser-known risks include the erosion of trust and damage the reputation of individuals and organisations.

THE PSTI REGIME HAS BEEN DESIGNED TO IMPROVE THE UK'S CYBER ATTACK RESILIENCE

In June 2018, hackers delivered an attack that harvested personal, passport and credit card information for nearly 500,000 British Airways passengers. Besides large fines from Britain's Information Commissioner, BA faced lasting reputational damage after the incident, falling from 31st to 55th in reputation score. This example also demonstrates how non-compliance with existing regulations is also a consequence of a data breach. Many industries have long-standing regulations and standards requiring the implementation of strong password policies to protect sensitive information and maintain data security. Failure to comply with these regulations can result in legal and financial penalties.

Compromised accounts resulting from weak passwords can lead to data breaches, exposing sensitive information such as personal data, financial records or intellectual property, so it's imperative to implement password policies that will protect businesses. Under the new UK law, if a user suggests a common password they will be prompted to change it on creation of a new account. But there are other proactive steps businesses can take.

BEST PASSWORD PRACTICES

Create strong and unique passwords using three random words. The best way to make a password difficult to hack is by using a sequence of three random words that are easy to remember. You can make it even stronger by including special characters and numbers, but don't fall into the trap of thinking that using symbols on short common words, eg "P@$$W0rd1" will make it harder to guess. Alternatively, consider using passphrases, which are longer and easier to remember than traditional passwords.

Whenever possible, enable multi-factor authentication (MFA) for your accounts to add an extra layer of security by requiring additional verification beyond just a password, such as a code sent to your phone or generated by an authenticator app.

Use different unique passwords for every email, social media and banking account. Store passwords in your browser when prompted, or use a password manager; both options are easier than remembering multiple passwords and safer than re-using passwords. Despite the fact that 91 percent of people say they know reusing the same password or a variation of it is risky, 66 percent still do it at least some of the time, if not all the time. This is why it's crucial for businesses to have guidelines for redundancy outlined in their password policies.

APPROXIMATELY 1 IN 10 EUROPEANS CLAIM TO HAVE EXPERIENCED ONLINE IDENTITY THEFT

Regularly updating passwords is especially important for accounts that contain sensitive information or are critical to business operations. Cyber security experts recommend changing important passwords every three months, but you should change your password immediately if your account is hacked, you're impacted by a data breach in any way, you have used an unsecure network or have discovered malware.

Regularly monitor accounts for any suspicious activity or unauthorised access. Enable notifications for login attempts, password changes and other account-related activities to alert you to any potential security incidents.

ISO 27001, formally known as ISO/IEC 27001:2022, an information security standard created by the International Organisation for Standardisation (ISO), provides a framework and guidelines for establishing, implementing and managing an information security management system (ISMS). According to its documentation, ISO 27001 was developed to: "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system." It includes password requirements that have been established as an international standard, ensuring passwords used by any organisation are strong, secure and regularly updated. Specifically, this standard defines rules and policies for choosing secure passwords and changing them regularly.

Having a standard for information security is no longer an optional extra, every single business or organisation needs a set level of information security. Because the most popular standard of security is ISO 27001, Evolve's approach to implementation has seen all our customers achieve the standard and maintain it. Not having an ISO 27001 Accreditation directly impacts how your customers and stakeholders perceive your business – ISO 27001 shows your customers that you are dedicated to ensuring your business is secure.

Poor password practices are an entirely avoidable mistake that cost businesses dearly every year. An estimated 81 percent of data breaches are caused by poor or reused passwords, and in 2022, the average cost of a data breach for organisations in the US was $9.44-million ($2.98-million for small businesses specifically). Stolen or compromised login credentials have already led to several high-profile data breaches in 2023, impacting businesses like PayPal, MailChimp, Reddit, Activision and others.

By following password best practices, businesses should be able to significantly improve their security posture and reduce the risk of data breaches and other cyber security threats. Moreover, implementing robust password policies demonstrates a commitment to security, which can enhance trust among customers, clients and stakeholders ●

Alan Stephenson-Brown is CEO at Evolve

In 2022 24-billion passwords were exposed by hackers