Concise Technologies

12 Ways

To Protect Your Business From Cyber Attacks

Businesses are much more aware of the dangers of cyber attack. Attackers are doing it for profit, and are organised. The damage to a business can be huge, in terms of loss of crucial data, reputational damage and even GDPR fines. Sadly, there is no single silver bullet to make your business secure from attack, however here are 12 steps that you can take to protect your business.

Step 1

Security Assessment

Many companies only have the vaguest awareness of the level of cyber threat and the degree of their exposure to it.

Get an assessment done that provides you with a written report of the vulnerabilities, the level of risk, and the options and costs of addressing those vulnerabilities. **You can't manage risks that you don't know about.**

Budgets are not unlimited, but with a security assessment, management can have visibility of the risks, prioritise the most severe, and have an agreed acceptance of the less severe risks.

Step 2

Spam and Malicious Emails

You should consider banning users from accessing their private emails on company PCs/laptops.

Email are one of the biggest vectors for cyber security threats, hiding attacks in attachments, links and the body of text itself.

Filter your emails for known spam/malware before they even reach your network.

Step 3

Passwords and Policy

Define and apply security policies on your network. Enforce rules about password length, complexity, and frequency of changing.

One area of vulnerability is the accounts of users who are no longer with the company being left in place. Make sure you have a defined leavers procedure that includes clearing down inactive accounts.

Password policies can be controlled by group policy and other third party software.

1/5 — Small businesses will suffer a cyber breach this year.

81% — Of all breaches happen to medium sized business

97% — Of breaches could have been prevented with today's tech

Step 4

Security Awareness

One handy tip for Office 365 is to upload a picture of your company log or office building, to be a background to the Office 365 login page for your users.

Periodic phising tests are a great way to train users away from being victims of a phising attack.

Train your users to spot malicious emails and phishing attacks. As well as improving your security, the provision of this training provides a big tick in the box when it comes to demonstrating GDPR compliance.

Step 5

Advanced Endpoint Security

We all know about anti-virus software, and how important it is to keep up to date.

The latest endpoint security goes beyond simple antivirus, to protect against file-less and script-based threats.

Endpoint protection is no longer limited to PCs and laptops, keeping mobile devices, like phones and tablets, up-to-date with anti-virus is a must in th modern day.

Step 6

Multi-Factor Authentication

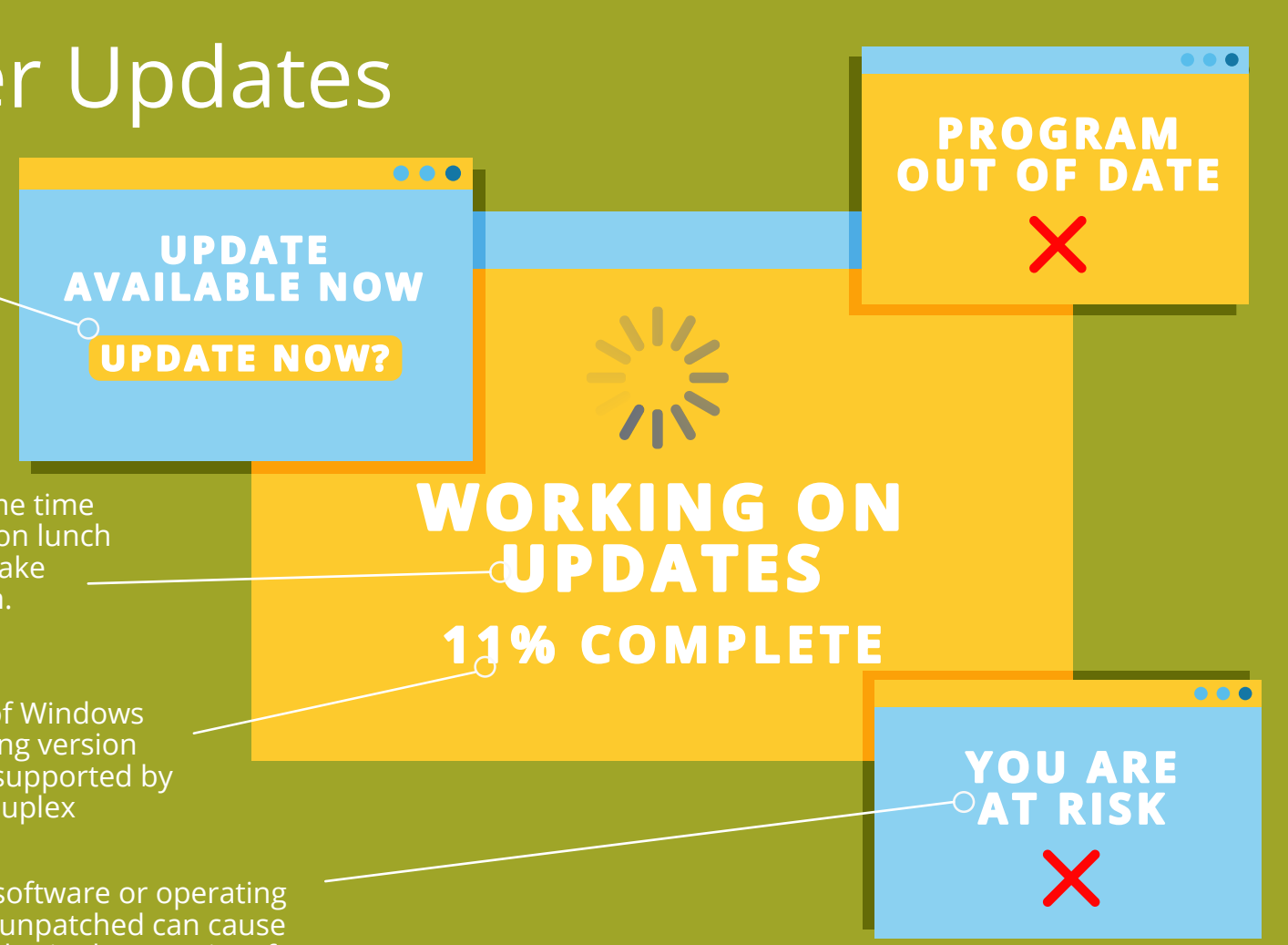
The problem MFA fixes is that if we are tricked into providing these credentials then an attacker can use them from any PC, anywhere in the worlds.

A simple form of MFA can be a free app on a mobile phone which sends out a one-time 6 or 8 digit code or a Approve/Deny push notification.

This should be used for wherever possible. It is a simple, inexpensive and effective way to ensure that even if your password gets stolen, your data will remain safe.

Step 7

Computer Updates



Software developers regularly release updates for their software. Microsoft, Java and Adobe release very regular updates as attackers target those the most.

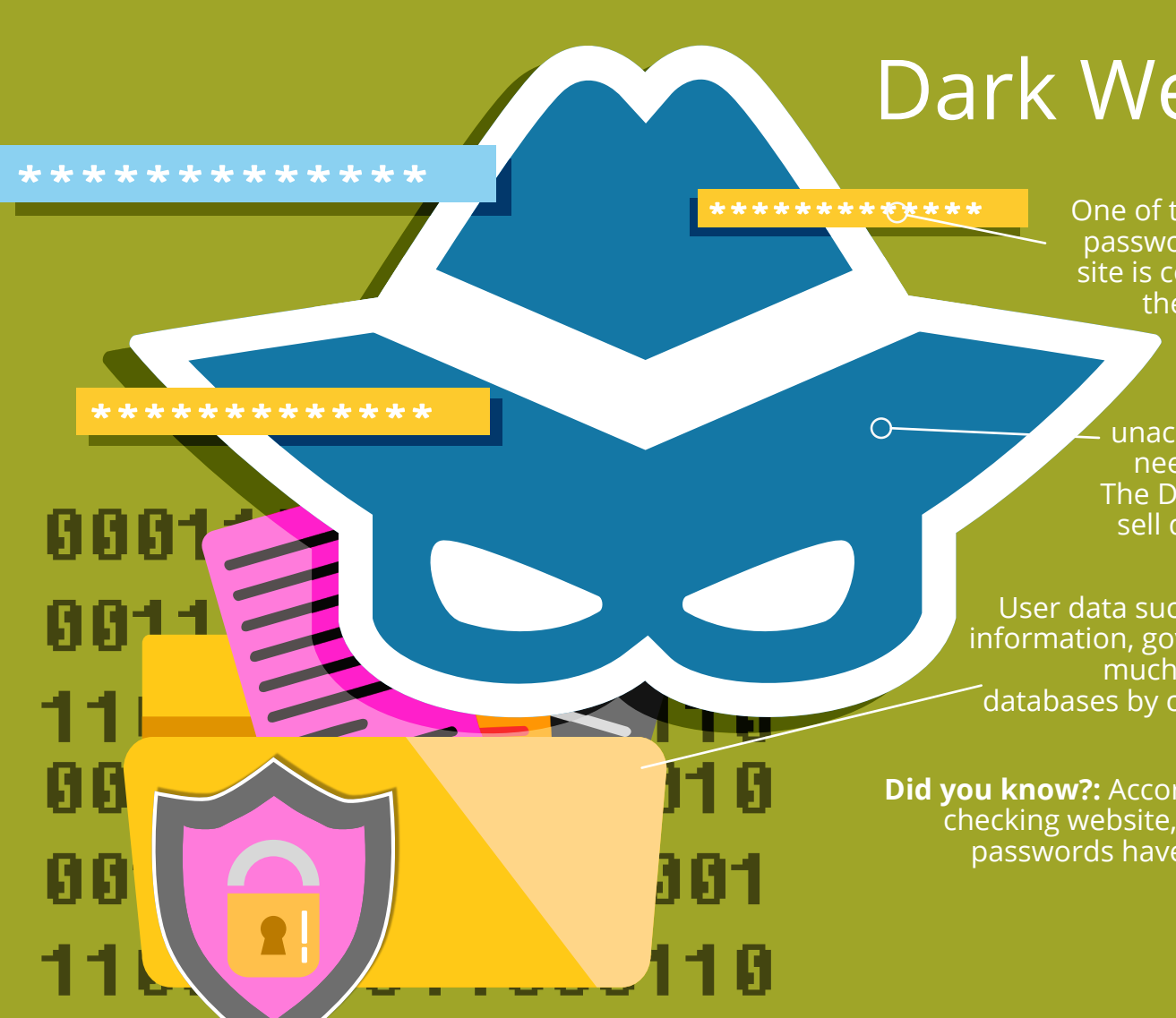
It is best to set aside some time for updates, this can be on lunch or after work. They can take some time to go through.

Did you know?: 25% of Windows 10 machines are running version 1903, which is now unsupported by Microsoft - Source Adduplex

Leaving software or operating systems unpatched can cause major holes in the security of your machine and business.

Step 8

Dark Web Research



One of the problems with using the same password for different sites is that if one site is compromised, the attacker will sell the password data on the dark web.

The dark web is a part of the web unaccessable to normal users due to it needing certain software to access it. The Dark Web is used to by criminals to sell data and illicit items without being traced.

User data such as passwords, names, payment information, government issued information and much more is breached from company databases by cyber criminals and distributed on the dark web

Did you know?: According to leading password breach checking website, Have I Been Pwned, 572,611,621 passwords have been exposed in data breaches.

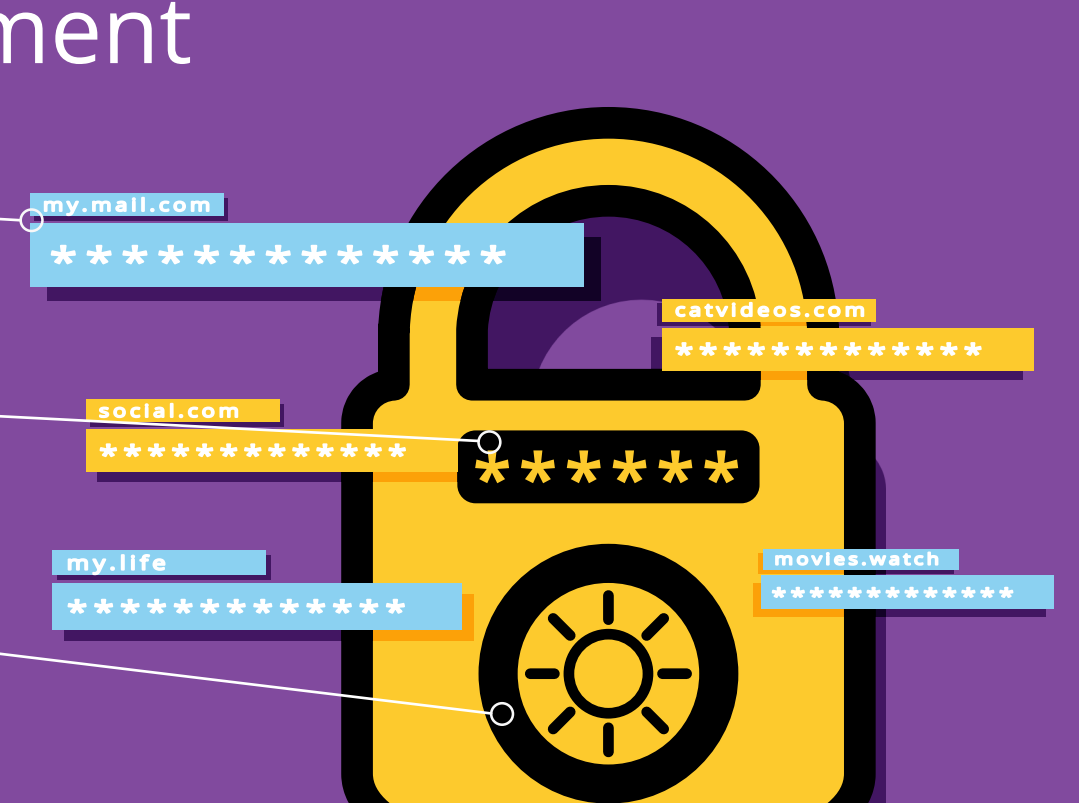
One small business is successfully hacked every 19 seconds

44% — Of UK consumers claim they willstop spending with a business after a breach

50% — Of cyberattacks in the UK involve phising.

Step 9

Password Management



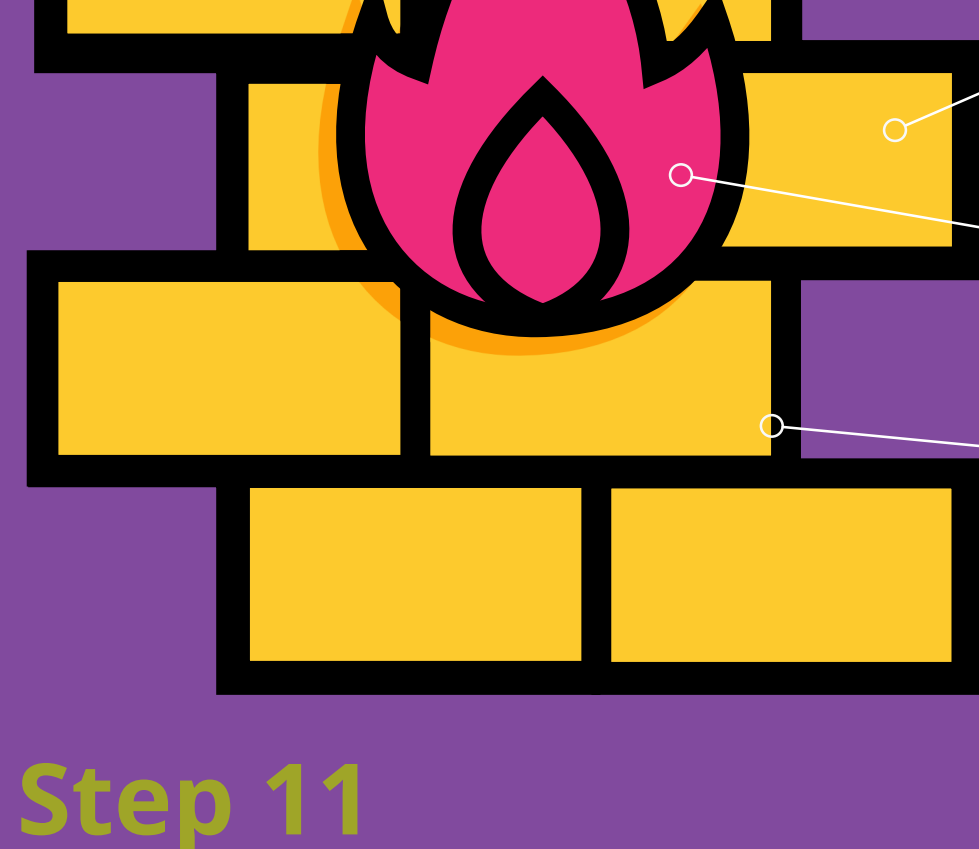
Our entire digital lives are hidden behind passwords these days. It is important to keep track of passwords while also ensuring they're kept safe.

Some password managers now offer a service to create a secure password and store it straight into it's vault.

There are many password managers available online now. It is important to choose a reputable manager to keep your passwords safe.

Step 10

Firewall



In security terms, your firewall is your front door. The firewall's job is to put a hard stop to threats that attempt to breach your network via open channels

It is imperative to keep firewalls up-to-date. Developers of firewalls are constantly providing new updates to devices to stop the ever-changing threats.

Detection and intrusion prevention features are a must for any modern, secure firewall.

Step 11

Encryption

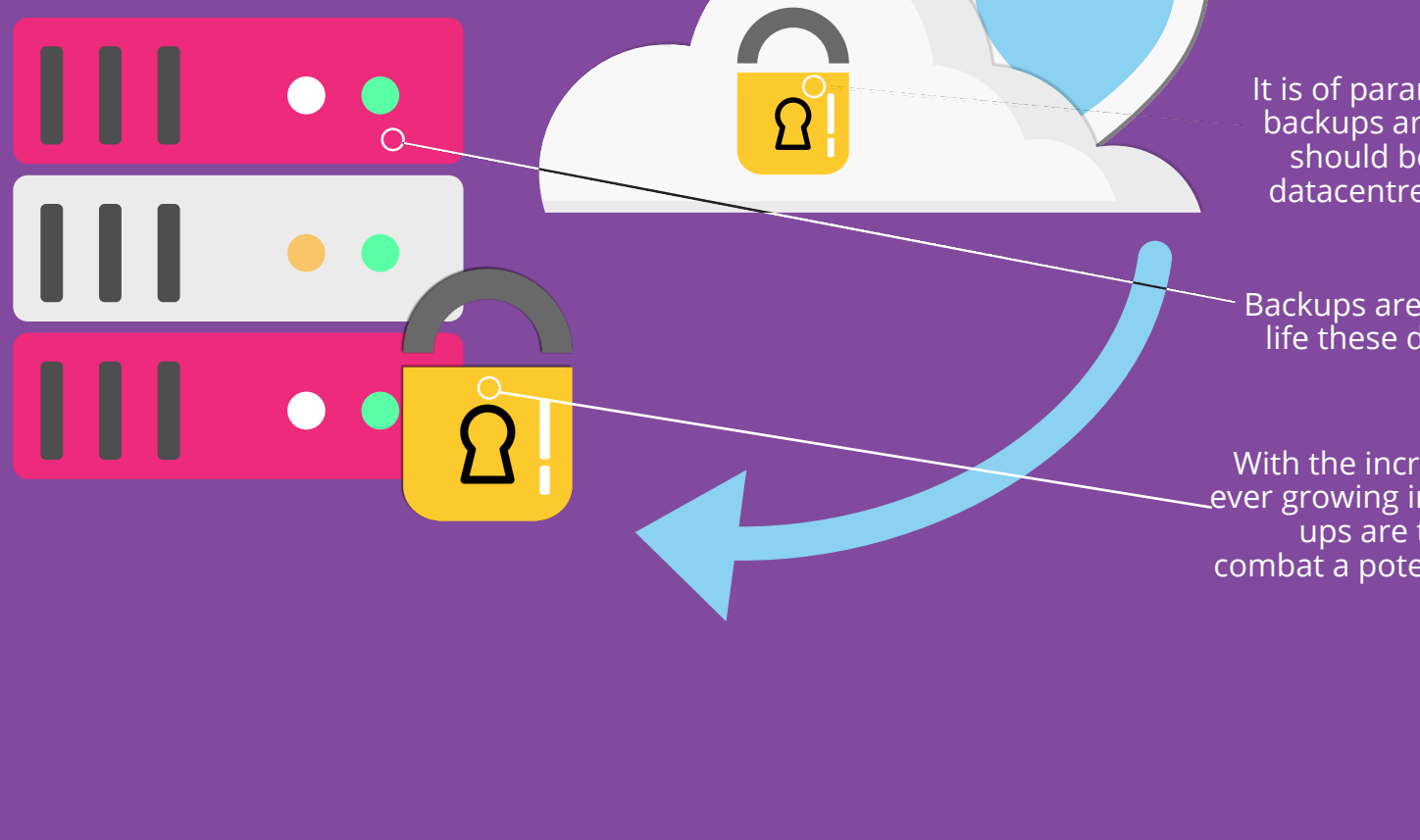
Encryption should be used when in rest (on one machine) and when in motion (transferred via email or messaging service)

Encryption refers to any process that's used to make sensitive data more secure and less likely to be intercepted by those unauthorized to view it.

There are lots of providers of hard drive encrytion with Windows offering a native hard drive encryption software available on their Window 10 machines called BitLocker.

Step 12

Backup



It is of paramount importance that backups are kept secure. Backups should be replicated to a secure datacentre that you trust and can hold accountability.

Backups are quintesential to home life these days, and even more so for business life.

With the increase of ransom attacks ever growing in the cyber-space, back ups are the ultimate weapon to combat a potentially business ending ransomware attack.