ENJOY SAFER TECHNOLOGY™

Top 10 tips for protecting your business

PROFILE
be smart with technology

www.profile.co.uk

Top 10 tips for protecting your enterprise customers

Protecting your business isn't a simple matter: businesses of every size are potential targets and every single one of your employees is a potential attack vector.

With that in mind, here are our **top ten tips** for securing your business and making your workforce your best defence.

1. Education

If your staff don't know what they are looking for how can they avoid it?

The vast majority of enterprise level hacks start with a phishing email. This could be a very specifically crafted email or a series of similar looking emails that are fired at as many people as possible in a scattershotapproach.

Either way if they don't know what to look out for or don't have a simplemethod of reporting any such activity then they are likely to get caught out.

A simple check list of what to look for in an email, how to confirmits authenticity and what to do if you spot a dodgy one, is a great start.

Phishing is just one example but it's a good starting point. Proper training and education could turn the weakest part of a company's defences, into the strongest.

So much comes back to good and regular staff education; this isn't the last you'll read about it.

2. Password policy

For passwords to be effective we need to remember them or have a means to remember them. Password managers can certainly help you control the strength of and access to certain passwords.

Mostbusinesslevelpasswordmanagerswill allowsharingof loginsinasecureenvironment withpermissionssettableforvaryinglevels ofaccess.Forexample,theaccountsteamwillbe logging into services that the marketing team will never need to use.

The two biggest problems are reusing the same password on multiple sites, or even easy to guess passwords.

Staff need to be educated on how to construct unique passwords from phrases or statements they are already familiar with, making small adjustments to suit the website and enabling them to reuse the base phrase with different modifiers.

3. Social Media policy

According to **research**, 40% of Facebook accounts and 20% of Twitter accounts claiming to represent Fortune 100 brands are fake.

The research claims that "social spam" has grown a whopping 658% since mid-2013 and that large brands experience at least one compromise on their social media channels every day.

At the very root of all this is good user education: understanding that links or media available through Facebook are not harmless and how these can lead to malware being allowed full reign on company networks due to one user "accidentally" trying to watch the latest cringe worthy celebrity fall out video.

Socialmediaisanexcellent toolwhenusedcorrectlybut accountsecurityhas tobeparamount, regular password changes are amust alongside regulated admin access that ismonitored.

Staff need to know what they can and cannot do on Facebook and fully understand how attacks happen and what to look out for.

4. OS updated

Keep systems up-to-date. It goeswithout saying hopefully, but this includes all of the software used on a daily basis.

Keeping the OS and antivirus up-to-date is incredibly important, particularly ensuring that updates are installed on every workstation in a timely manner.

On a tangential note, if a workstation or a member of staff doesn't require Adobe Flash Player or Java then get rid of them. Particularly Flash, as it is consistently shown to be vulnerable to zero-day exploits, even after brand new updates.

5. VPN, public Wi-Fi

For the mobile workforce using public Wi-Fi in service station coffee shops or hotels might be a necessity, but it could also be exposing them to attack.

For example, "DarkHotel" used phony update packages to install malware on high value targets while they stayed at luxury hotels.

The phony updates were for popular services like GoogleToolbar, Adobe Flash and Windows Messenger.Allowingtheupdatesto downloadopensthesystemuptomalware;specifically targeting usernames and password for common services it seems.

The bestway to avoid this and otherWi-Fiman-in-the-middle style attacks is to use a VPN or virtual private network.

6. Multi-factor authentication

Two Factor Authentication is a means to protect private login credentials. The problem with usernames and passwords is that they are easily lost or stolen and in some cases you may not actually be aware that you have been compromised.

By taking something that we know (username and password) and then adding another securing feature like a 'one-time passcode' (OTP) you can further protect that login from guesses or brute force attacks.

A 'brute force attack' refers to someone repeatedly trying to guess a password. Usually this would be performed by a computer rather than an individual: very powerful computers could potentially guess millions, if not billions, of potential passwords per second.

The passcode can be sent by SMS text, email, generated on a smartphone or small device called a token whenever login isattempted.

Usually thecodewillhavealimitedlifespanbeforeitexpires, isuniqueandcanonlybeused once.A newcode is generated every time you try to login so even if the usernames and passwords are compromised, without the OTP the login will fail.

7. BYOD policy

Bring Your Own Device, or BYOD, requires a clear understandable policy, outlining security requirements and best practice that all staff should read, understand and sign.

Educate and train as much as possible, knowing and understanding why and how threats can expose the business is a much better way to protect data.

Antivirus must be installed (with regular scans).

Ensure that updates are installed as quickly as possible, particularly in the case of large-scale vulnerabilities like Meltdown and Spectre. All apps should be periodically reviewed with some limitations on free apps and the ability to install them.

8. Proper permissions

Ensuring that your employees have the permissions they need and only the permissions they need can go a long way to mitigating a potentially successful phishing attempt or any intrusion into your system: even the dreaded 'insider threat'.

For example, does the marketing department need access to the technical departments systems? Looking even closer, does your socialmedia guru need access to your business marketers' customer information?Unlikely.

The more aggressive you can be the better. Obviously, you don't want to hamper your staff's day-to-day working but knowing who has access to what and occasionally reviewing permission is essential.

9. Updating old systems

An OS reaching End of Life (EoL) can have a massive impact in terms of replacement/upgrade cost, or cause a massive vulnerability if they aren't replaced/upgraded.

The negative PR backlash due to exploits and vulnerabilities would be extensive and fairly damaging to the brand, so they will do all they possibly can to keep you safe: it's in their best interest to do so.

However, running out-of-dateWindowsXP opens you up to any exploits that are found or currentlyknown.

Of course, you can install internet security, be very careful what emails you open and what web pages you go to, but it's like putting the most expensive locks on your 3-ply shed hoping that will keep its contents safe.

Updating your operating systems is not all about keeping Microsoft afloat, it's one of the multiple layers required inmodern day computer security.Think of it like the foundations for your nice shiny new house:without it everything could crumble down around your ears.

10. Data Compliance

In May 2018 GDPR changed everything for anyone who holds personal data.

Previously the **ICO** can fine up to £500,000 for serious breaches of the Data Protection Act, although to date, we have only seen a couple of fines up around the £400,000 figure.

From May 2018 we could see fines of up to **£17 million, or 4% of global turnover** of the previous financial year.

Encryption is a big part of protecting data. It will protect against USB's, laptop's or DVD's left on trains, lost in the post or just lying around for anyone to view.

Data loss is not just about leaving a USB or Laptop on a train, it might also include someone reading information they should not see while in your very building.

Conclusion

That rounds up 10 quite simple ways to secure your business.

There are of course many other tips we could list here, as security is always a multi-layered discipline that evolves over time, but this will form a solid foundation and should keep all but the most determined cyber criminals at bay.

Founded in 1992, ESET is a global provider of security software for enterprises and consumers dedicated to helping the world fight against evolving computer threats. ESET's award winning products rank among the world's most advanced security solutions. ESET Endpoint Antivirus, our flagship product, consistently achieves the highest accolades across a host of industry leading comparative tests and is the foundational product that builds out the ESET solutions line. ESET is headquartered in Bratislava, Slovakia with offices in the UK, Germany, USA, Czech Republic and Singapore. ESET delivers superior security solutions to customers in over 200 countries across the globe.

ESET's extensive line of solutions protects across all platforms from workstations and servers to mobile devices, helping our clients maintain maximum protection across all types of environments. The superior detection capabilities and low system requirements of our solutions have been, and continue to be, recognised by independent anti-malware testing organisations. Since testing began in 1998, our antivirus is the only solution worldwide that has never missed a single "In the Wild" virus and holds the world record for VB100 Awards.