Be cyber-aware;

our guide to keeping your business safe

Whether we like it or not digital technologies and online services have and are continuing to revolutionise our lives.

From online banking, to grocery shopping, to taxing our car, registering for tax-free childcare to completing our Self-Assessment of Service Statement (SASS), for it to be the platform from which we teach our children (Hwb), to listening to music or simply socialising with our friends. We interact with technology in so many ways, that we don't even realise we're doing it.

"The UK's digital economy currently accounts for around 10% of GDP, and ICTs contributing significantly to productivity growth.

"As we emerge from the recession, the Welsh Assembly Government sees the Digital Economy as a central element in Economic Renewal: a new direction, offering businesses across Wales opportunities to innovate and grow. As we now enter a period of tightening public finances, we also see digital technologies at the heart of transforming public services, helping deliver better and faster services at lower cost. Everyone should have the ability and opportunity to enjoy the benefits digital technologies offer. Securing digital inclusion is vital for our future."[1]

Like the real world, the online world also comes with risks, but there is no need to let that put you off using it to help grow your business.

In this article, we guide you through the essentials of online safety - we alert you to the basics of cyber-security, how to recognise threats and explain why you need to be aware.

How secure is your computer? tablet? phone? Yes...phone.

Most of us forget that our mobile phones are mini-computers, most of our day-to-day business is probably conducted using our phones; banking, social media, emails etc. They are our life support machines. Yet many of us don't protect them.

Rule #1: Passwords

First things first...are your digital devices password protected?

By this we mean have you locked your device at the front screen? Choosing to not password protect your devices is the digital equivalent of leaving your front door unlocked. According to a report published by CBNC in 2014, 34% of Americans do nothing to protect their smartphone.[2]

You should make it as difficult for someone to pretend to be you as possible. Don't use obvious passwords such as your user name, real name, date of birth, names of family members or simple sequences like 'abcdef' or '123456'. Always try to include an upPer-case letter, a speci@l character and/or some number5.

howsecureismypassword.net is a handy tool to check your password strength. We wouldn't recommend typing in your real passwords but something similar instead to gain an insight into how strong it is.

Be smart and use different passwords for different websites and change them regularly, but try not to make them so complicated that you can't remember them. If you must write them down don't store them on your devices or on a sticky note next to your computer.

Also, avoid having your devices "remember" your passwords. Especially those that are portable or are used by different people.

The 10 most commonly used passwords of 2016:

1. **123456**
2. **123456789**
3. **qwerty**
4. **12345678**
5. **111111**
6. **1234567890**
7. **1234567**
8. **password**
9. **123123**
10. **qwertyuiop**

* Source: Keep Security

Rule #2: Have you installed antivirus software?

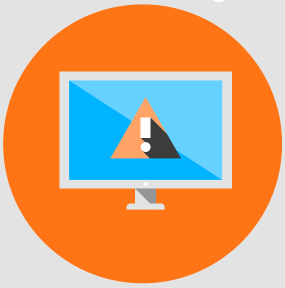
Make sure you have an antivirus/anti spyware software installed.

There are plenty on the market such as Norton or McAfee, but there are also lots of free antivirus software packages such as Windows Defender which comes pre-installed with genuine Windows packages from Version 8 onwards. It's also worth checking with your bank, depending on the type of account you have you may have a free subscription waiting to be taken advantage of.[3]

Most threats to your digital device/s will appear in the form of malicious software (malware) or viruses so it is important they are kept out. Make sure you keep the antivirus software up to date and run regular security scans.

Don't be lulled into a false sense of security if you have Apple products. Whilst Apple is generally considered more secure than Windows they still get viruses and need to be protected.

Rule #3: Update regularly



Make sure you are using the most up-to-date versions of all software and operating systems.

They include important security updates to protect your data. Many software programs will alert you to this when connected to the internet. If you're not sure then visit the 'Action Center' setting in the Control Panel of your computer, for phones & tablets this function is likely to be found in Settings.

Watch out for 'Microsoft Scam Calls'. If you receive a call from a security 'expert' offering to fix your PC, it is a scam. Microsoft or any other IT support company such as Talk Talk or BT, will never call you unexpectedly 'regarding a problem with your computer'.[3]

Rule #4: Back up your data

We all know how frustrating it can be when our devices become old.

They run slow, crash without warning etc. Not only that, with them being so portable they are more likely to be damaged or stolen. It is therefore important to make sure you can access your files from anywhere via a secure online server or cloud system. You may also like to make a physical back up - to a portable hard drive or memory stick. This should then be kept off-site in case of theft, fire or another unexpected emergency.

Rule #5: Secure your wireless network

By securing your wireless network with a password prevents unauthorised individuals trying to access your network. Even if it is to access the free Wi-Fi!

Rule #6: Don't talk to strangers

We teach the children in our care not to talk to strangers. We too, should be wary when being asked to divulge sensitive information online. Use your common sense. If something seems suspicious then it probably is.

Double check the validity of any email sent to you containing a request for personal information, a link or attachment. Do you know the sender? Double check the email address. Trust no-one...hackers are very good at making an email look like it's come from an official source (including Amazon, PayPal or eBay). Hover your cursor over the link, this will reveal the actual address.

If you receive an email or phone call from your bank for example, informing you of any suspicious activity on your account. Always call them to check the validity of this using official contact details held on file. Your bank will never ask you to reveal personal data such as PIN's, passwords or ID numbers.

Spam emails are a fact of life. We all receive them, don't be alarmed if you receive an email claiming to be about your account with HSBC when you don't bank with them for example. Simply delete.

Rule #7: Consider your environment

Most of us like the idea of being able to take ourselves away from our normal work environment and catch up with our emails over a nice caffé latte in our local coffee shop instead.

However, this is not without its hidden dangers. Not only would we advise that you make sure your work is hidden from view of prying eyes but that there is also the potential for your data to be intercepted if you are connecting to public Wi-Fi. Considering using a Virtual Private Network (VPN) instead.

Rule #8: Watch your pennies

When processing payments for goods or services received pay attention to the details on the invoice.

It is possible for a fraudster to impersonate a supplier or client. If an instruction is received advising of new bank details by email, telephone or letter it is important that you call the supplier or client back using the contact details you have on file to double check.

Bank payments in the UK are processed by a sort code (6-digits) and an account number (8-digits). The name on the account is not routinely checked.

It is not only money being paid out you need to be mindful of. It is also money coming in. Potential fraudsters will often issue overpayments by cheque, BACS or CHAPS, then acknowledge their mistake by asking you to simply send them the difference. Always make sure the payment clears first, which is unlikely.

This is also a common way of money laundering. Fraudsters will deposit dirty money into your account and you will wash it for them by sending it back. If in doubt, contact the Financial Crime team at your bank before responding to any requests.

Rule #9: Not everyone wants to be your friend

As much as we like to share those special moments in our lives with our friends we need to be careful as to how much information we put out there into the public domain.

It wouldn't take a criminal long to build up a fake profile of you from an open Facebook account. Date of birth, the number of your new front door, where you work etc. Ensure your account can only be viewed by accepted friends.

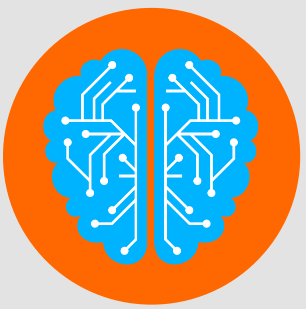
Barclays recently broadcast an excellent advert to illustrate this: **https://youtu.be/w2tW50CD6Aw**

Rule #10: Knowledge is power

Share this list of tips with your team. It is important that they follow similar procedures with their own devices.

Do not allow unknown devices to connect to your network, this is how viruses spread. Consider setting up a guest network for staff and visitors rather than allowing them to access to your private network.

By ensuring all staff computers have an admin access, you will reduce the risk of software being installed by accident. The admin control challenges updates, it is recommended that only your IT support team and/or manager have admin access.



Conclusion

By following these basic security controls you will significantly reduce the risk of a cyber & data attack. There is however, a wealth of guidance out there on how to keep your business safe when online if you wish to look into it further.

If you are unsure, then there can be no replacement to seeking out the expertise of professionals who can assist you with regular testing of networks and systems, as well ensuring you are compliant with all legalities from a data protection perspective.

Further reading:

- **digital.wings.uk.barclays** – tools and tutorials to help boost your knowledge. Anyone can register.
- **www.cyberaware.gov.uk/cyberessentials** - Government backed and industry supported scheme to guide businesses in protecting themselves against cyber threats.
- **actionfraud.police.uk** – the UK's national fraud and internet crime reporting centre
- **www.bbc.co.uk/webwise** - packed full of easy to understand resources to give your digital skills a boost

References:

[1] http://bit.ly/2wJzovM
[2] http://cnb.cx/2eH7RR5
[3] http://bit.ly/23IXxhf
[4] http://bit.ly/2xMQ9Tp