PriorityIT
Put your business first

Call: 01225 636000
Email: info@ PriorityIT.co.uk
Web: www.priority-it.co.uk

Top Tips for online safety

Do you know how to spot a scam? Take the quiz:
https://phishingquiz.withgoogle.com/

1 Password safety

Don't use simple passwords

Simple passwords can be cracked automatically using a word list.

You can test the strength of a password on this website: How Secure Is My Password

Never reuse passwords on multiple website or services

If one website or service is breached by hackers, then they will have access to any other website that used the same password.

Regularly Change your password

Changing your password ensures if someone does have your password it's not for long. Many scams that steal passwords may lie dormant for a period of time before someone logs in to see what they can do with your information.

You could use a password manager like Dashlane or RoboForm which create and store secure passwords

Setup 2FA/MFA

This is two factor, or multifactor authentication - on any online service you use, such as Facebook and Paypal. Most online services allow you to set up 2FA/MFA, this is where once you have logged in with your username and password another code is requested, normally from your phone. This means that if anyone gets your password, they also require physical access to your phone.

2 Keep your online personal self separate from your online business self

Privacy tools on Facebook can be used to lock down your personal profile.

Do you have a Backup of your critical data?

A lot of data can be lost if you are the victim of a Cyber Attack e.g. CyrpoLocker. This threat can be mitigated if you have a good backup.

Do you have a backup? Has it been tested?

3 Keep your data safe

Check if you have been a victim of a data breach

There have been many high profile data breaches which disclosed details such usernames and passwords – TalkTalk, Sony Playstation, LinkedIn and BA among them. Depending on the data breach, your username and passwords may be on the Dark Web. To find out, go to this Experian web page.

Be careful what you upload to the internet

Once it is there. It is there forever! Certain sites allow you to delete things, but other sites index them so that anything deleted can be uncovered.

4 Invest in good anti-virus software

Anti-virus software such as Eset now offer Web Protection and the software will recognise and block scam websites.

5 Don't rely on the SSL padlock symbol as a symbol of trust

SSL certificates are free for anyone and having one does not mean the site is 'safe'. It simply means the data is encrypted. Fraudsters are now using legitimate services to hide behind, or simply creating their own SSL Certificate.

6 Watch out for scams

Be suspicious of emails that ask you to login to a service when clicking a link

Most scam emails we see are designed to steal your email password, so always double check the web address of sites asking you to log in. If in doubt, close the browser and log in by typing the web address yourself.

Microsoft or other companies e.g. BT Talk-Talk etc.. will NEVER call you to tell you your computer is infected with a virus

These are scam phone calls designed to scare you to pay for their services and to steal your personal information.

Beware free software downloads

We have seen many viruses originate from someone downloading and installing a 'free version' of software (examples are Microsoft Office or a DVD Converter). Nothing's free - especially software which can cost hundreds of pounds.

Be suspicious of emails and calls asking you to transfer money

If you are asked to transfer money via email or if a supplier or client tell you they have changed bank details, follow up via a telephone call to the requestor to confirm. Don't reply to the email, as it's likely you will be communicating with the fraudster as the fraudster may have access to the mailbox.

Follow us on Twitter for more tips: @ PriorityIT