How to keep your business safe online

During these difficult times BT are helping to keep the nation connected with a range of Top Tips on Tech. The following suggestions can help you keep your business safe online.

Tip 1: Identifying different types of cybercrime

There are lots of different types of cybercrime that you and your business could be susceptible to. It's important to know how to identify them as they could lead to anything: from your personal data being stolen, to your website going down and you losing business, to losing your customers' data.

Malware:
These are viruses and spyware that can be used to gather valuable information like passwords, or even credit card numbers without you even knowing.

Ransomware:
This is a variation of malware, which locks you out of your own data, then demands payment to regain access.

Brute force attacks:
Cybercriminals bombard your website or online accounts with lots of password combinations to try and gain access.

DDoS attacks:
Distributed Denial of Service attacks are designed to take down your site using a flood of internet traffic.

Phishing:
Another common way to try to steal protected information is phishing. You can find more information from us on phishing, by going back to BT.com/Tech-Tips.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT
BEYOND
LIMITS

Tip 2: How to protect yourself and your business

Although cybercrime can be hard to spot, there are a number of ways to make sure you stay protected against it.

Update software:
It may sound simple, but always make sure your operating system and programs are up to date. When you update any of your devices new features can be added, and outdated or faulty features will either get fixed or removed.

Usually your device will send you a notification to inform you when a new update is available and it's important to install the update without delay to keep your business safe. Automatic updates are a great way of making sure your devices stay up to date.

Antivirus software:
Make sure you have it installed, switched on and have the automatic update feature turned on to keep you safe from the latest viruses.

Passwords:
Create a different strong password for each account. A good idea is to pick three random words and use a mixture of case, numbers and symbols.

Multi-factor authentication:
It sounds complicated but it just means using more than one way to prove it's you. It's usually a combination of things like: something you know, like a PIN or a secret question; something you have with you, like a card or token; or physical proof, like a fingerprint or retinal scan.

For more Top Tips on Tech
visit: BT.com/Tech-Tips

BT BEYOND LIMITS

Tip 2: Continued

Prevent DDoS attacks:
Contact your webpage host to make sure your account is secure against these type of attacks.

Regular backups:
You may already do this, but a regular back up is crucial to make sure you always have a copy of your important files and info. You can back up to the cloud or an external hard drive, but remember to password protect the drive if you use one.

Document shredding:
Don't forget to shred important documents at home, just like you usually would in the workplace. Cybercriminals will use any information they can – they don't have to start online.

Unwanted attachments:
Under no circumstances should you open up any email attachments that you were not expecting or are from senders that you do not trust, as these could include embedded malware.

Keep your employees informed:
It is important to keep your staff up to date on security regulations and laws. The Information Commissioner's Office (ICO) provides excellent information on this topic, to help you understand your and your customers data rights.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS

Tip 3: What to do if you are hacked

You've prepared for the worst, but if the worst happens and you do get hacked, what do you do? Here are a few ways to spot that something's wrong and what you can do about it.

Unusual activity:
Look out for inquiries or questions from companies you've never used, keep an eye on financial outgoings and call your bank immediately if something looks odd. Also, check your emails and post for any business correspondence that you didn't set up.

Damage limitation:
If you suspect a breach or attack, change your passwords and disconnect your device from any networks. It's the quickest and easiest thing you can do to stop further problems.

Protect customer data:
Remember that you need to protect any customer data because of GDPR, the General Data Protection Regulation.

If you experience a data breach, it's your responsibility as a business to tell your customers and inform the Information Commissioner's Office (ICO) as soon as possible.

Please share these tips with other business owners to make sure we're all protected from cybercrime.

For more Top Tips on Tech visit: BT.com/Tech-Tips

BT BEYOND LIMITS