Stay safe online - blog six - protecting your computer

Blog

05.01.23

Protecting yourself when you go online is a necessity. With a world of information accessible at your fingertips, it is easy to get caught up in the ease of accessibility and on-demand information available. However, you don't want your personal details to be easily accessible to everyone else. Our 'stay safe online' blog series will share tips that you can utilise going forward to protect yourself when interacting with the online world.

Today's blog will cover:

Why is it important for your computer to stay safe?

There are many ways you can keep your computer safe, and it is important to do so. Without the right protections, computers can be hacked, giving access to all your information - whether online or not. However, it is not just information that can be accessed if someone gains entry to your computer. Webcams and microphones can be vulnerable, meaning that not just your online activity can be monitored.

What is malware?

Malware includes viruses, Trojan horses, spyware and worms. These are all designed to gain access to your personal information or damage your computer. If your computer is connected to the internet, it is vulnerable to malware. The two main ways a computer can get infected is through the internet or email.

How does my computer get infected?

Phishing email scams are not just used to steal your personal information. They can also contain malware. By disguising the emails as if they've come from a legitimate source and encouraging the receiver to click the link. Websites that are not secure can hide malware, and you don't need to actively download something for it to infect your computer.

However, downloading content on file-sharing sites, or from untrustworthy sources, is the easiest way for malware to infect your computer. Many forms of malware are also able to use a variety of methods to infect other computer systems, spreading out across networks, social media, and emails.

How do I avoid a malware attack?

The first step is to make sure your computer's antivirus software is up to date. If your computer is not already protected, look into the best software for you or your organisation. It is also advisable to update your operating systems, browser and plugins so that they are running to the latest version and are more robust against attacks. The best way to ensure your computer is up to date is to turn on 'auto updates' for windows and for your browser. Using strong passwords and two factor authentication where possible will also help protect you and your computer from malware.

The next step is to be cautious when clicking on links on sites that aren't considered 'top-level', such as .com, .net, .edu, .co or .org for example and to avoid clicking on pop ups that don't relate to site content, such as adverts. Don't open attachments in emails from unknown senders or with suspicious content.

It is also advisable not to use any USBs or other external devices unless you own them or trust who they came from.

What do I do if I think my computer is infected?

There are numerous signs that your computer might be infected. This list, from the Federal Trade Commission, covers many of the common symptoms of infection, such as if your computer:

- suddenly slows down, crashes, or displays repeated error messages
- won't shut down or restart
- won't let you remove software
- serves up lots of pop-ups, inappropriate ads, or ads that interfere with page content
- shows ads in places you typically wouldn't see them, like government websites
- shows new and unexpected toolbars or icons in your browser or on your desktop
- uses a new default search engine, or displays new tabs or websites you didn't open
- keeps changing your computer's internet home page
- sends emails you didn't write
- runs out of battery life more quickly than it should

Should you notice any of these symptoms, run a scan through your antivirus software. This should identify and be able to remove most common malwares. Once you are certain that your computer is infection free, it is advisable to change all your passwords again, in case any were accessed and stolen.

At this point, you should also back up your computer and your files. Some malware attacks can delete documents and photos. To ensure that in the event of a possible future attack you don't lose these files, it is recommended to regularly back up your computer either on an external hard drive or an online backup service.

If you get any communication from TAB that seems strange or out of place please contact us immediately to make sure before entering any personal information.

Stay tuned to read more about staying safe online in this blog series.

This online blog series is an introduction to online safety and is designed to raise awareness of the challenges of interacting online. This article is for information only and does not constitute advice or a personal recommendation. When it comes to online activity it is important to be cautious and seek appropriate professional advice.

Capital is at risk. Property values can go down as well as up. Borrowers may default and investments may not perform as expected. Interest and income are not guaranteed. Returns may vary. You should not invest more than you can afford to lose. TAB is not authorised by the Financial Conduct Authority. Investments are not regulated and you will have no access to the Financial Services Compensation Scheme (FSCS) or the Financial Ombudsman Service (FOS). Past performance and forecasts are not reliable indicators of future results and should not be relied on. Forecasts are based on TAB's own internal calculations and opinions and may change. Investments are illiquid. Once invested, you are committed for the full term. Tax treatment depends on individual circumstances and may change.

You are advised to obtain appropriate tax or investment advice where necessary. Understand more about the key risks here.

TAB is a trading name of TAB London Limited. Registered in England and Wales with registration number: 11225821 and whose registered office is at 101 New Cavendish Street, London W1W 6XH.