Get Safe Online Global24

Online Survival Guide

We've come a long way since we launched in 2006. But the message is still simple: keep control and protect yourself and your assets.

Get Safe Online is a pioneer in internet safety. It was one of the first resources in the UK and, indeed the world, for the public and businesses to go to for advice on how to protect themselves, their families, their finances, devices and workplace on the internet. Not only from scams, but various kinds of abuse and other online harms. We continue to be highly regarded by all who know us, not only in the UK but in numerous countries around the world via websites and local representation.

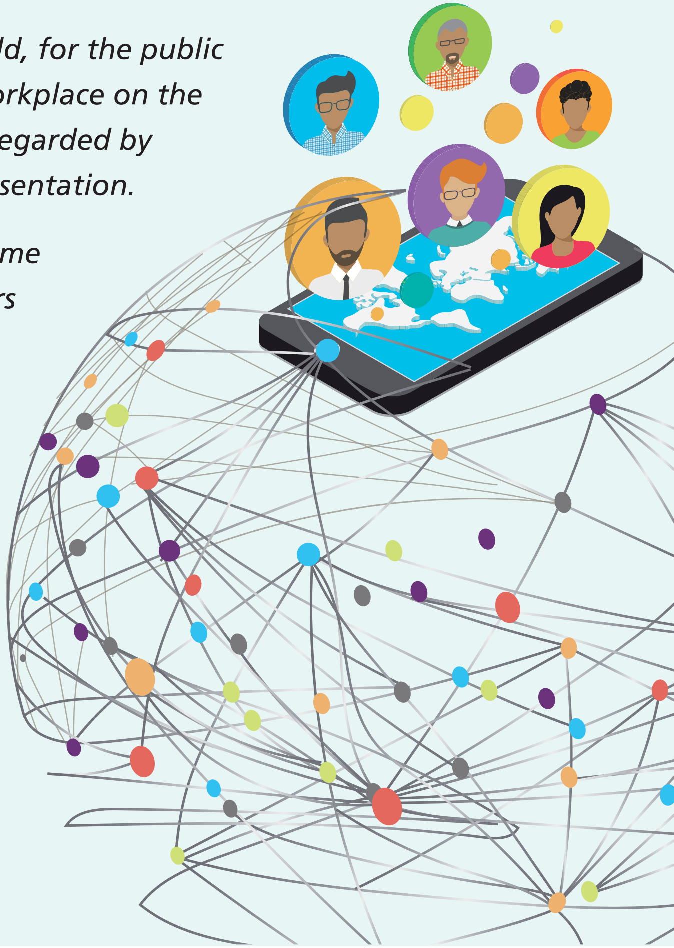
Unfortunately, during the ensuing decade and a half, criminals have become far more sophisticated. In the same time, the fight against cybercrime has also taken quantum leaps. However, our own positive online behaviours have proved to be the most effective protection against those who want to do us harm. That's why this year's flagship Get Safe Online Global24 event is focused on taking a back-to-basics look at online safety with some great tips from our experts.

It also comes as we depend on the internet to work, play, communicate and transact as never before, due largely to COVID-19. Alongside the uncertainty and upset caused by a global pandemic, a perfect storm has been created for cybercriminals and abusers.

On behalf of my colleagues at Get Safe Online, I'd like to introduce our Online Safety Survival Guide for individuals and businesses, thank all of our valued partners and others who are supporting the event, and also to urge you to read and pass on our tips to loved ones, friends and colleagues.

Tony Neate

Chief Executive Officer, Get Safe Online



Get Safe Online Global24

Foreign, Commonwealth
& Development Office

It has been fantastic working with Get Safe Online over the last two years to help implement the Commonwealth Cyber Declaration, to ensure all Commonwealth countries share the benefits of new technology safely.

Get Safe Online is a highly respected organisation, delivering expert and independent advice to individuals and businesses in the UK, and has ably replicated that advice in, to date, another 22 countries around the world.

Our partnership during the UK's term as Chair of the Commonwealth has so far reached substantial numbers of people in the Caribbean, the Pacific and Africa, promoting good practice to keep them safe online.

With our virtual world growing during the Coronavirus pandemic, it is more important than ever to be alert to the threats posed by cyber criminals.
I am pleased to commend this Online Survival Guide to ensure more people can take advantage of the internet safely and securely.

William Middleton
Director, Cyber & Tech Security
Foreign, Commonwealth & Development Office

Get Safe Online Global24

The Online Survival Guide, developed for our Get Safe Online Global24 event, takes a back-to-basics look at how we can all help to protect ourselves from online harms, in both our personal and business lives. Please read these tips from our online safety experts, and pass them on.

Your top tips for keeping safe online

- Choose, use and protect **passwords** carefully, and use a **different one** for every online account in case one or more get hacked. Try using three random words and strengthening them with numbers, symbols and combinations of upper and lower-case letters.
- Ensure you always have **internet security software** (often called anti-virus/anti-spyware) loaded on computers and a similar app on your mobile devices, and that this is kept updated and switched on. Remember that **smartphones and tablets can get infected** in a similar way to computers.
- Always apply **updates to operating systems and software** on your computer and apps on your mobile devices. Many include vital security updates to avoid hacking or malware.
- Never assume that **Wi-Fi hotspots** in places like cafés, bars and hotel rooms are secure, so don't use them when you're doing anything confidential online. Instead, use your data, a mobile broadband modem (dongle) or if it's for work, a VPN (virtual private network).
- Always consider that online or on the phone, **people aren't always who they claim to be**. Fake emails, texts and phone calls are a favourite way for fraudsters to approach their victims.

For full information and advice, visit **www.getsafeonline.org**

Get Safe Online Global24

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

Your top tips for keeping safe online

- **Don't click on links** in emails, posts, tweets of texts – and **don't open attachments** – if the source isn't 100% known and trustworthy, or it seems strange that you'd be receiving them.
- **Never pay for anything by direct bank transfer** – including goods, services, tickets, travel and holidays – unless it's to someone you know personally and is reputable.
- Never reveal too much **personal or financial information** in emails, on social networking and dating sites and in person. You never know who might see it, or use it.
- **Always report** fraud or abuse to the appropriate authorities.

There are also two other golden rules you should remember: **think twice,** because everything may not be as it seems, **and if it seems too good to be true, it probably is.**

For full information and advice, visit **www.getsafeonline.org**

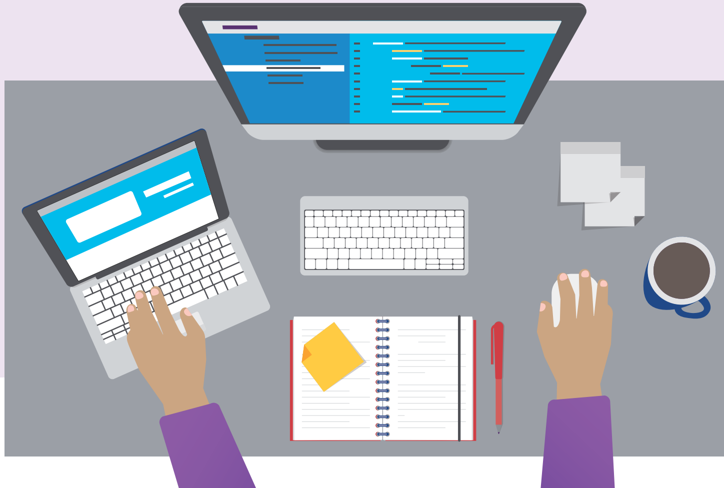
GET SAFE ONLINE

Get Safe Online Global24

COMMONWEALTH
UNITED KINGDOM CHAIR-IN-OFFICE

Your top tips for keeping your business safe online

- Choose, use and protect passwords carefully, and use a different one for every account.
- Ensure that reputable internet security software is loaded on computers and security apps loaded on mobile devices, and kept updated and switched on.
- Never reveal too much personal or financial information … you never know who might see it, or use it and you can never be sure who's asking.
- Don't click on links in emails, texts or social media posts, or open email attachments if the source isn't 100% known and trustworthy. Remember that cybercriminals are highly devious and can even spoof sender email addresses and phone numbers.
- If you get an email or other communication requesting an unusual payment, or re-direction of a payment to a different bank account, always call the company on the phone number you know to be correct to check the request is authentic.
- Always keep software, apps and operating systems updated, as updates often contain security fixes. If you can, set programs and apps to update automatically.
- When you or colleagues are out and about, never use Wi-Fi hotspots in places like cafés, bars and hotel rooms for anything confidential, as they may not be secure, or even fake hotspots. Use your data, a mobile dongle or VPN instead.
- Take your time and think twice, because everything may not be as it seems.



For full information and advice, visit **www.getsafeonline.org**

Other things you should do to safeguard your business

- Run regular online safety and information security awareness sessions for all employees. Get staff to question and challenge things that seem irregular.
- Ensure that only those who need it can gain physical access to computers and servers.
- Enforce strict access to company, employee and customer data.
- Perform regular backups to a reputable service, preferably one that is in the cloud and easily accessible when you need it.
- Introduce and reinforce rules about mobile devices, including keeping them safe, use of public internet and secured home access, and the use of employees' own smartphones and tablets in the business.
- Make sure you and all staff can spot the signs of a social engineering email or phone call designed to gain confidential information and know how to avoid company being defrauded in this way.
- Have a software policy firmly in place including usage, updates, licences and what to do with redundant programs and apps.
- When disposing of redundant computers, servers and mobile devices, ensure all data is thoroughly erased (not just deleted) to ensure it doesn't fall into the wrong hands.
- Set guidelines about employees' social media use to help ensure that the reputation of the business is not compromised.
- If your business enables access to its systems by others in the supply chain, take steps to ensure that they have robust technology and processes in place.