

**With our tips, a safe online  
Christmas is a piece of cake.**



[www.getsafeonline.org](http://www.getsafeonline.org)



**Renfrewshire**  
Council



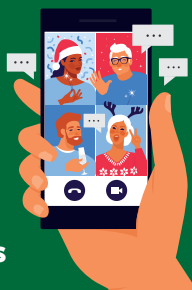
# Your top tips for a safe online Christmas.

You can find more information at [www.getsafeonline.org](http://www.getsafeonline.org)



For many of us, the festive season is the most eagerly anticipated time of the year for adults and children alike. Traditionally a time of getting together with friends and family and giving and receiving gifts, Christmas and New Year now have a modern twist, thanks to online technology.

Whether it's shopping or socialising, playing games or watching a movie, the internet now has a major part to play in most people's Christmas. This makes it essential that we take precautions to protect ourselves, our families, finances and devices against online harms.



**#OnlineChristmas**

If you think you've been a victim of a scam, report it to **Action Fraud**, on **0300 123 20 40** or at **[www.actionfraud.police.uk](http://www.actionfraud.police.uk)**  
In Scotland, call 101.

## Buying online

Learn how to spot the difference between genuine and fake websites, secure and insecure payment pages and authentic and counterfeit goods. Before you visit a website, check if it's likely to be legitimate or fraudulent using our **Check a website tool**.

Beware of texts claiming to be from a parcel firm telling you there's a 'delivery fee'. If in any doubt, **always call the organisation** on the number you know to be correct.

## Connected devices

Protect all new or second-hand internet-connected phones, tablets and computers with a **reputable security app/software**. Add a new **PIN or passcode** as soon as you power up. Ensure all devices are **backed up** automatically so you don't lose your precious documents and photos. Check **privacy and location settings** for new and existing devices ...that's yours and your family's.

Always set up new **passwords on internet-connected devices** like voice assistants, appliances, cameras, kids' toys and fitness watches, as soon as they're switched on. Using the factory-set default passwords could result in them being hacked. Always use different passwords for different devices, websites or accounts for the same reason. And remember ... **voice assistants** are designed to hear everything! Find more information about **setting up connected devices**.

## Updates

**Download updates** to software, apps and operating systems on all your devices as soon as you get notified. Better still, set them to update automatically. Otherwise, they could get infected by malware, leading to fraud or identity theft.

## Mobile apps

Download those new apps **only from official sources** such as App Store, Google Play or Microsoft Store. Getting them elsewhere could result in fraud or identity theft.

## Gaming

Avoid oversharing, griefing, in-game overspending and pirated games. Keep track of how much time you're spending online. **Keep an eye on your kids' gaming**, check on games' PEGI age limits and talk to them about who they're or playing and chatting with.

## Pre-owned mobile devices

**Do a factory reset** to erase your data if you're selling or gifting a computer, mobile device or console. You can find out how from the manufacturer's website. If you've bought or been given a used device, remove the previous owner's settings and data if this hasn't already been done.

## Oversharing

Make sure **what you share online** is respectful and doesn't reveal confidential, sensitive or embarrassing information about yourself or others, including family

members and friends. If you're away from home, keep it to yourself, as social media is a burglar's best friend.

## Out & about

Don't use **Wi-Fi hotspots** in cafés, pubs, hotels, on public transport and other public places for anything confidential as they could be either insecure or fraudulent.

## Protecting your family

**Talk to your children** about being safe and responsible online, including what they share, who they're talking to and the type of content they access, including apps and games. Consider downloading a respected parental control app and using ISP content filters. Make sure your children aren't running up bills in games and other apps.

## Video calls

Make sure video calls are **safe and secure** by using a service that needs a strong password, and don't share the call invitation or details outside the person or group on the call.



For more information on how to stay safe online this festive season, visit [www.getsafeonline.org](http://www.getsafeonline.org)

# Get Safe Online

Get Safe Online is the UK's leading source of information and advice on online safety and security, for the public and small businesses. It is a not-for-profit, public/private sector partnership backed by law enforcement agencies and leading organisations in internet security, banking and retail.

For more information and expert, easy-to-follow, impartial advice on safeguarding yourself, your family, finances, devices and workplace, visit [www.getsafeonline.org](http://www.getsafeonline.org)



[www.getsafeonline.org](http://www.getsafeonline.org)



**Renfrewshire**  
Council

## OFFICIAL PARTNERS

**TESCO**

**first direct**

**NatWest**

**HSBC**

**ROYAL AIR FORCE**

**ARMY**  
BE THE BEST

**Royal Bank of Scotland**

**M&S BANK**

**LLOYDS BANK**

**HAUFAX**

**BANK OF SCOTLAND**

**creativevirtual**  
The source of conversation™

**CITY OF LONDON POLICE**  
National Fraud & Cyber Crime Reporting Centre

**NPCC**  
National Police Chiefs' Council

**NATIONAL TRADING STANDARDS**  
eCrime Team

**cifas**  
The UK's Fraud Prevention Gateway

**EUROPOL**  
EC3 | European Cybercrime Centre

**neighbourhood ALERT**

**Uywodraeth Cymru**  
Welsh Government

**ActionFraud**  
National Fraud & Cyber Crime Reporting Centre

**METROPOLITAN POLICE**

**Ofcom**

**VS VICTIM SUPPORT**

**EUROPOL**  
EC3 | European Cybercrime Centre

**neighbourhood ALERT**

**Uywodraeth Cymru**  
Welsh Government