

# Your online safety do's and don'ts

- Choose, use and protect **passwords** carefully, and use a different one for every online account or website.
- Always have **internet security software** (antivirus) loaded on computers and a similar app on your mobile devices.
- Always apply **updates** to operating systems, software and apps on computers and mobile devices.
- Don't use public **Wi-Fi hotspots** for doing anything confidential.
- Don't click on **links or attachments** unless you're 100% sure they're known and trustworthy.
- Being asked to pay for goods or services by **bank transfer** could be a sign of fraud.
- Never reveal too much **personal or financial information** in emails, posts, on websites or phone calls.
- Remember that **not everyone online is who they seem**.
- **Think twice** before you click.
- If it seems **too good to be true**, it probably is.



Brought to you by



Ambassador  
Scheme



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