Radfield
Home Care

What if your loved one is at risk online? A guide to digital safety for families

The digital world has become an essential lifeline for staying connected to the people and passions we love. At **Radfield Home Care**, we believe in helping our nation age well by keeping people connected to the things that matter most.

Whether it's a video call with a grandchild in another time zone, browsing local history archives, or managing a weekly grocery shop, the internet offers incredible opportunities for independence and enrichment.

However, as the online landscape evolves, so do the risks. For many families, a nagging worry persists: *is my loved one safe?* We understand that this concern comes from a place of deep love and a desire to protect.

How to keep your family safe online

Navigating digital safety isn't about restricting freedom; it is about providing the right tools and knowledge to ensure that your family members can explore the web with confidence and security.

Within this guide we'll go into the basic tips on digital safety for families, how to identify and avoid common online scams & fraud, social media privacy & security, and where to find relevant support.

Radfield
Home Care

Devices, passwords, and basic protection

Before diving into the complexities of social media, digital safety begins with the hardware in our hands. Ensuring that a device is set up correctly is the first line of defence against external threats.

Software updates and security

One of the most effective ways to protect a loved one online is to ensure their devices, be it a tablet, smartphone, or laptop, are running the latest software. Manufacturers frequently release updates that patch security vulnerabilities.

We recommend enabling automatic updates on all connected devices so that these vital protections happen in the background automatically, without requiring manual intervention.

The power of passwords

We often see people using the same simple password for every account, which creates a significant risk. If one account is compromised, they all are. We suggest moving away from names and dates of birth toward **passphrases** - three random, unrelated words joined together (e.g., *TeapotCarMountain*).

To make life easier, consider:

- **Password Managers:** These secure **digital vaults** store all passwords, requiring the user to remember only one master key.
- **Biometrics:** Using a fingerprint or facial recognition is often much simpler and more secure than typing a complex code. All your data is stored as encrypted text - no copyable 'images' of your biometric data is actually stored
- **Two-Factor Authentication (2FA):** This adds an extra layer of security by **sending a code** to a mobile phone when logging in from a new device. Most trusted websites and tools utilise this feature and it's the easiest way to bolster your security and avoid online fraud.

Securing the home network

The Wi-Fi router is the gateway to your home. Ensure your home network is password-protected and that the default password provided by your provider has been changed to something unique.

Radfield
Home Care

How to navigate online communication and social media safety

Social media is a wonderful tool for preventing isolation. It allows our loved ones to see photos of family outings and engage with communities of shared interests. However, these platforms require a mindful approach to privacy.

Social media privacy settings are key

When helping a loved one set up a profile on platforms like Facebook or Instagram, the first stop should always be the social media **privacy settings**. We recommend setting profiles to "Private" or "Friends Only." This ensures that personal updates and photos aren't visible to the general public or searchable by strangers.

Sharing with care

It is important to have gentle conversations about what is appropriate to share. **Oversharing personal details** - such as a home address, phone number, or even updates about being home alone - can inadvertently provide information to those with ill intentions. Our Care Professionals often help clients engage with technology safely, encouraging them to share memories while keeping sensitive data private.

Friend requests and connections

A good rule of thumb is to only accept friend requests from people known in "real life." If a request comes from a familiar name but seems out of character, it's worth a quick phone call to verify it's actually them before clicking "Accept."

Recognising common digital scams, fraud, and manipulation

Scammers are becoming increasingly sophisticated, often using emotional manipulation (often referred to as **Social Engineering**) to gain trust. At Radfield Home Care, we are a champion for care that people want as well as need, and that includes protecting the financial and emotional well-being of those we support.

Common online scams and fraud to watch for

- **Phishing Emails, Calls and Texts:** These often appear to be from reputable and trusted organisations like the NHS, HMRC, or a bank. They usually create a sense of urgency, claiming there is a "problem with your account" or a "refund waiting."

- **The "Grandchild in Trouble" Scam:** A distressing and often convincing message, often via WhatsApp, claiming to be a family member who has lost their phone and needs money urgently for an emergency.
- **Investment and Romance Scams:** These involve long-term manipulation, where individuals build a false sense of intimacy or promise high returns on "exclusive" investments to extract money over time.

How to spot common digital scams and fraud

We encourage families to teach the **Stop, Challenge, Protect** framework:

1. **Stop:** If a message feels urgent or suspicious, take a moment. Genuine organisations will never pressure you to act immediately.
2. **Challenge:** It is okay to ignore or refuse requests. Only criminals will try to rush or panic you.
3. **Protect:** If you think you've shared sensitive information, contact your bank immediately and report it to **Action Fraud**.

Monitoring safely while respecting independence

One of the most delicate balances to strike is ensuring safety without infringing on a person's dignity or independence. No one wants to feel watched, but everyone deserves to be safe.

Open communication over surveillance

Rather than installing intrusive monitoring software without consent, we advocate for an **open-door policy** regarding digital life. Ask your loved one what they enjoy doing online. Share your own experiences, including mistakes you've made or weird emails you've received. Making digital safety a shared family topic removes the stigma and makes it easier for a loved one to come to you if they feel something is wrong.

Collaborative safety for your family

If a loved one is living with cognitive changes or simply feels overwhelmed by technology, you might agree to:

- **Shared Account Access:** Having access to online banking or primary email accounts to "keep an eye" on unusual activity, provided this is agreed upon and documented via a **Power of Attorney** if necessary.

- **Notifications:** Setting up bank alerts for transactions over a certain amount can provide peace of mind without requiring a constant review of private statements.

The role of Care Professionals

Our **Care Professionals** are trained to support individuals in a way that promotes independence. They can assist with basic tech troubleshooting or provide a "second pair of eyes" when a suspicious email arrives, always acting with the utmost respect for the individual's privacy and choices.

Trusted resources and ongoing support

Digital safety is not a one off task; it is an ongoing journey. As technology changes & develops, staying informed is all of our best defence.

Where to turn for help

There are several excellent organisations dedicated to digital safety in the UK:

- **Age UK:** Offers fantastic guides on making the most of the internet and staying safe.
- **Get Safe Online:** Provides practical advice on every aspect of digital security.
- **Action Fraud:** The UK's national reporting centre for fraud and cybercrime.
- **The National Cyber Security Centre (NCSC):** Offers the "CyberAware" toolkit for individuals and families.

Building a support network

At **Radfield Home Care**, we see ourselves as a vital part of your support network. We are here to help your loved ones stay connected to their community, their family, and the wider world. By combining family vigilance, professional support, and the right digital habits, we can ensure that the internet remains a source of joy and connection rather than anxiety.

The digital age should be inclusive. By taking these steps, you are empowering your loved one to enjoy the modern world safely, avoid online fraud, and keeping them connected to the things that matter most.

Discover more with Radfield Home Care

Radfield Home Care

If you are looking for support that prioritises independence, connection, and safety, we are here to help. Our dedicated Care Professionals provide tailored support that respects the unique needs of every individual.

FAQs

What are the most common online scams targeting older people?

The most frequent scams in the UK include "Phishing" (emails/texts pretending to be from banks or the NHS), "Grandparent scams" (urgent WhatsApp messages claiming to be a relative in need), and "Remote Access scams" where callers claim your computer has a virus to gain control of your device.

How can I tell if a website is safe to use?

Always check the address bar for a padlock symbol and a URL starting with ‘https://’ (the ‘s’ stands for secure). Look for spelling mistakes in the web address and use the "Stop, Challenge, Protect" framework before entering any financial details.

Should I use a password manager for my elderly relative?

Password managers are highly recommended as they remove the burden of remembering multiple complex codes. They secure all accounts behind one "Master Key" or biometric (fingerprint/face) login, significantly reducing the risk of account takeovers.

Radfield
Home Care

How do I report an online scam in the UK?

If you or a loved one has been targeted, report it to **Action Fraud** at 0300 123 2040 or via their website. If money has already been lost, contact your bank immediately using the number on the back of your debit card to freeze your accounts.

Can social media be made safe for older parents?

Absolutely. By setting profiles to "Private" and "Friends Only," you ensure only trusted individuals can see posts. Families can also use "Shared Access" to help monitor messages and friend requests, ensuring the platform remains a tool for connection rather than a risk.