digitalreflow

Staying Safe on Social Media

Social networking is a global revolution, enabling around a billion people worldwide to stay in touch with their friends, share experiences and photographs and exchange personal content. The key word here is PERSONAL. There is a sense of the untouchable when it comes to social media. This is a dangerous sentiment. For all of social media's positives and innovations, its accessibilities must be respected and not to be trifled with.

This will explore the best practices to utilise all the unequivocal positives about social media but also the dangers people can encounter.

Getting Started

Never disclose private information when social networking Be wary about who you invite or accept invitations from Think very carefully before being persuaded or harassed into changing your basic beliefs or ideologies Be careful about clicking on links in an email or social networking post

Various social networking sites are also valuable tools used by many companies and individuals to extend their contacts and deliver marketing messages. The nature of social networking – having such an enormously engaged base of users who are unknown to you – means that using it carries a degree of risk including becoming a target for cyber-criminals.

The Risks

- Disclosure of private information by either yourself or friends/contacts
- Bullying
- Cyber-stalking
- Access to age-inappropriate content
- Online grooming and child abuse
- Encountering comments that are violent, sexual, extremist or racist in nature, or offensive activities and hateful attitudes
- People trying to persuade or harass you into changing your basic beliefs or ideologies, or adopt an extremist stance
- Prosecution or recrimination from posting offensive or inappropriate comments
- Phishing emails allegedly from social networking sites, but actually encouraging you to visit fraudulent or inappropriate websites Friends', other people's and companies' posts encouraging you to link to fraudulent or inappropriate websites
- People hacking into or hijacking your account or page
- Viruses or spyware contained within message attachments or photographs
- You or a family member posting that you're away or going away on holiday and therefore advertising that your home is empty.

Safe Social Networking

You can avoid these risks and enjoy using social networking sites by following a few sensible guidelines:

- Do not let peer pressure or what other people are doing on these sites convince you to do something you are not comfortable with.
- Be wary of publishing any identifying information about yourself – either in your profile or in your posts – such as phone numbers, pictures of your home, workplace or school, your address or birthday.
- Pick a user name that does not include any personal information. For example, “joe_glasgow” or “jane_liverpool” would be bad choices.
- Set up a separate email account to register and receive mail from the site. That way if you want to close down your account/page, you can simply stop using that mail account
- Use strong passwords.
- Keep your profile closed and allow only your friends to view your profile.
- What goes online stays online. Do not say anything or publish pictures that might later cause you or someone else embarrassment.
- Never post comments that are abusive or may cause offence to either individuals or groups of society.
- Be aware of what friends post about you, or reply to your posts, particularly about your personal details and activities.
- Remember that many companies routinely view current or prospective employees’ social networking pages, so be careful about what you say, what pictures you post and your profile.
- Don’t post your holiday dates - or family photos while you are away - as social networking sites are a favourite research tool for the modern burglar.
- Learn how to use the site properly. Use the privacy features to restrict strangers’ access to your profile. Be guarded about who you let join your network.
- Be on your guard against phishing scams, including fake friend requests and posts from individuals or companies inviting you to visit other pages or sites.
- If you do get caught up in a scam, make sure you remove any corresponding likes and app permissions from your account.
- Ensure you have effective and updated antivirus/antispyware software and firewall running before you go online.
- These points will not completely protect you from the many dangers the cyber world can throw up. There is very little that will provide entire absolution but reducing risk is the name of the game. Stay vigilant. Stay alert and ultimately stay safe.