

Staying safe on social media

Phishing on social media

Phishing is the fraudulent practice of sending messages purporting to be from reputable companies to induce individuals to reveal information, such as passwords and credit card numbers. They will quite often include a link which, if clicked on, will take you to a phishing website or infect your computer with malware. The way to protect yourselves and RCOT from being phished on social media is to do the following:

- Never accept a friend request from an account that looks suspicious: It might only have a couple of followers, or the posts from the account might seem like they are written by a bot.
- Never click on links requesting personal information: Reputable social media platforms will never ask users to click on a link to update their personal details.
- Use unique login details for each account: It's best to always use unique details for each platform so that in the unfortunate event of being phished, the attackers won't have access to your other accounts.
- Two-factor authentication: Most social media platforms have made two-factor authentication mandatory now. It adds that extra layer of security from cyber-attacks. Information on how to set these up on each platform is available:
 - [Facebook](#)
 - [Twitter \(X\)](#)
 - [LinkedIn](#)
 - [Instagram](#)
 - [TikTok](#)
 - [Threads](#)
 - [YouTube](#)

If a security breach has taken place, or you suspect one, please let the [Technology Experience Partner](#) know immediately. Read our [Cyber security policy](#).

Negative comments

If a post is receiving negative commentary (one negative response or more) then RCOT's reputation may be at risk. Each case will be different and will need a separate discussion on the best course of action.

If you deem the risk low level, discuss it with your line manager or relevant stakeholders and decide on a suitable course of action. If you deem the risk high, and/or you've received more than one negative comment, then contact the [Social Media Lead](#) for advice on how to respond and monitor.

Do not delete the post or comment unless asked to do so by the Social Media Lead; this can be seen as an admission of guilt and won't necessarily solve the issue.

Online abuse

Online abuse can come in several formats:

- **Cyberbullying:** Sending threatening/nasty messages or other communications to people via social media.
- **Cyberstalking:** Persistent unwanted contact from another person – either someone you know or a stranger.
- **Trolling:** Intentionally upsetting, shocking or winding up selected individuals, groups of people or a more general audience who are usually people not known to the troll.
- **Creeping:** Persistently checking up on someone on social media by browsing their timeline, updates, conversations, photos/videos, profiles and friends.
- **Doxxing:** A type of harassment that takes place when someone gets hold of personal information about you – such as your name, address, job, other personally identifiable data, health information or financial details – and posts it on the internet without your consent.

More information on types of online abuse, and how to avoid and report them to the appropriate authority, is available from [Get Safe Online](#).