

Top Six Security Safeguards

Small actions that make a big impact. Keeping our systems and data secure is everyone's responsibility. Follow these six simple habits every day to protect Coterie and you.



1. Only install approved software

Does your agency have an approval process? Before installing anything make sure you check that it is secure. This also goes for free tools and extensions.



2. Know who IT support is

If your team has IT support, make sure you familiarize yourself with them and the ways they will contact you.

If anyone else reaches out claiming to be IT:

- Do not engage.
- Do not install anything.
- Do not grant access.



3. Slow down with emails

Phishing is still one of the most common risks.

Before clicking a link or opening an attachment, take a few seconds to check:

- Do you recognize the sender and email address?
- Were you expecting this message?
- Does anything feel off in tone or urgency?



4. Use strong, unique passwords and a Password Manager

Never reuse passwords. Avoid anything easy to guess.

A password manager is there to make this easier. It helps you create and store strong, unique passwords for every account.



5. Never approve unexpected MFA requests

If you receive a multi-factor authentication (MFA) prompt you did not initiate:

- Do not approve it.
- Deny the request.
- Report it immediately.

This means someone may be trying to access your account.

Also, never share MFA codes with anyone, even if they claim to be from IT.



6. When in doubt, report it

If something feels off, report it to your IT team or superior.

That includes:

- Unusual emails
- Unexpected requests
- Strange pop-ups
- Logins you did not initiate