STAFF GUIDE

Safe Sharing and Privacy

How to handle a suspicious message without exposing anyone.

Before sending a suspicious message or screenshot to anyone

- Remove names, addresses, phone numbers, account and order numbers.
- Remove passwords, codes, card details, QR codes, and login links.
- Defang web addresses in anything public.
- Do not forward a private conversation without permission.
- Send private material through the approved route only.
- Never ask a child, client, or victim to open a suspicious site.
- Do not accuse anyone on the strength of one screenshot.

A report or a feed match is a lead, not proof.

Partner privacy contact

Who to ask inside your organization	[PARTNER NAME / CONTACT]

For scam warnings, go to
watchout.report

Cybersecurity Reach Foundation
501(c)(3) nonprofit

YOUR LOGO, NAME AND PHONE