



Working With Us

Posters, a session for your group, a route for your students, and somewhere to write. What we ask, and what we do not do.

Four things we offer

- Posters and print material for the places your community already stands and waits.
- A session on recognising scams, for your students, your staff, or the people you serve.
- A real route into this career for students who want one.
- An email address anyone can write to with a scam question.

Posters and print material

Large-format warnings written for people who are not technical, free to print as many times as you like. You add your own organization's name and contact details in your browser before printing; nothing is uploaded to us.

- Six posters covering the patterns people meet most: paying to get a job, sharing a code, being rushed, paying before verifying, and stopping before you click or tap.
- One-page handouts, including what to do when something has already happened.
- Newsletter and email copy, written to be pasted as it is.

A session for your group

We can run a session on how scams actually reach people and how to recognise them, pitched at whoever is in the room: students, staff, parents, or older members of a community.

- Roughly an hour, and it works as a class, a staff meeting, an assembly, or a community evening.
- It is built around recognition rather than fear, and it uses real patterns we have investigated.
- Remote sessions are the easiest for us to commit to. In person depends on where we can get to and when.
- Ask before you schedule anything, so we can be honest about what we can deliver and by when.

For students who want this career

Twelve weeks, about five hours a week, remote and free. Students do real work rather than shadowing: investigating, checking claims against evidence, and writing clearly, so it is open to students who are not technical. They finish with a piece published under their own name and a written reference. Students under 18 are welcome, with guardian consent and mentor conversations that are never one-to-one and unobserved.

- They apply at cybersecurityreach.org/volunteer and pick an area: investigation, reporting and curation, AI and data, software, or events and education.
- Four to six students at a time, because every piece of their work is read and answered by a person.
- Ask us for the Student Research Program sheet, which covers it properly.

Somewhere to write

Anyone can email help@cybersecurityreach.org with a general question about a suspicious message, website, or call. Your members do not need to be technical to ask, and they do not need to go through you.

- Nobody should send passwords, one-time codes, private messages, identity documents, or banking details. We do not want them.
- It is a general guidance service, answered by people, not an emergency line and not case handling.
- There is also a free checking tool at cybersecurityreach.org/check that walks someone through a suspicious message on their own.

What we ask of you

- Put the material where the people you serve will actually see it.
- Check the date on a warning before you share it, and take it down when it has passed.
- Keep our wording as it is. It is written to be understood by people who are not technical.
- Tell us what your community is actually seeing. That is the only way our material gets better.

What we do not do

We are not an emergency service, a bank, a lawyer, or a safeguarding team, and we do not handle cases. If someone has lost money or is in danger, they need local help first. Keep using the reporting and support routes your organization already trusts.

Working with us outside the United States

The scams we track are international. Fraud does not stop at a border: the same fake delivery message, the same fake job, and the same fake login page turn up in different countries with the words changed. Our sources are global and our material is written for the pattern rather than for one country's brands.

What is local is reporting and recovery. Those routes differ everywhere, and getting them wrong would send someone to the wrong place, so we do not advise on them. Pair our material with the reporting route your organization already trusts.

Starting

There is nothing to sign, nothing to pay, and no account to keep. Everything is at cybersecurityreach.org/partners. Write to info@cybersecurityreach.org, tell us who you serve, and say which of the four you want to start with.

For scam warnings, go to
watchout.report

Cybersecurity Reach Foundation
501(c)(3) nonprofit

YOUR LOGO, NAME
AND PHONE