



Protecting Yourself from Phone & Email Scams

Community Safety Information

Hello,

Scams are becoming more convincing. A phone call may look like it is coming from your bank. An email may use the logo of Social Security, a delivery company, or another organization you know. A caller may even know your name, address, or other personal information.

The most important thing to remember is this: you do not have to decide whether a message is real while you are on the phone or looking at the email. You can stop, step away, and ask for help.

If you are ever unsure, talk to someone on the Otwarte Circle team before giving information, sending money, clicking a link, or allowing anyone access to your computer or phone.

The scams we are seeing most often

Bank and account security alerts

A caller, email, or text may claim there is suspicious activity on your bank or credit-card account. They may tell you to move money to a “safe” account, provide your password, or read back a one-time security code.

Do not do it. A security code sent to your phone is meant for you. Do not give it to an unexpected caller. Hang up and contact your bank using the number on the back of your card or another number you already know is correct.

Government and law-enforcement impersonators

Scammers are pretending to be from Social Security, the IRS, local police, the FBI, courts, and other government agencies. They may say you missed jury duty, there is a warrant for your arrest, your Social Security number has a problem, or your money is connected to a crime.

They may sound official and may even make the caller ID look legitimate. Government and law-enforcement agencies do not call or text you to demand payment by gift card, cryptocurrency, wire transfer, cash, or courier.



Fake Social Security emails

There has been a recent increase in fraudulent emails that look like Social Security communications and claim to provide access to a Social Security statement. A link in the message may lead to a fake website designed to steal personal information.

If an unexpected Social Security email asks you to click a link, do not use the link. Go to Social Security through a website or contact method you already know is legitimate.

Unpaid toll messages

A text or email may say you owe a small toll and must pay immediately to avoid late fees, a suspended registration, or another penalty. These messages often imitate real toll agencies.

Do not click the link in the message. If you think you may owe a toll, contact the toll agency independently using information you find yourself.

Package and delivery messages

You may receive a message saying a package cannot be delivered because your address is incomplete or a small fee is due. The message then asks you to click a link and enter personal or credit-card information.

If you are expecting a package, go directly to the delivery company's official website or app and enter your tracking number there. Do not use the link in an unexpected message.

Computer and tech-support scams

A pop-up, email, or phone call may say your computer has a virus or your account has been hacked. The person may ask you to download software, give them remote access to your computer, or call a number shown on the screen.

Do not give an unexpected caller control of your computer, phone, or accounts. Do not call a phone number from a frightening pop-up. Close the message and ask for help.

Family emergency and AI voice scams

Technology can now be used to imitate a person's voice. A caller may sound like a child, grandchild, friend, or someone else you know and say there has been an



accident, arrest, medical emergency, or other crisis. They may beg you not to tell anyone.

Hang up and call your family member directly using the number you already have. If you cannot reach them, call another trusted family member. Urgency and secrecy are warning signs.

A simple rule: STOP. HANG UP. DON'T CLICK. CHECK.

STOP.

Do not give personal information, passwords, account numbers, Social Security numbers, security codes, or payment information to someone who contacted you unexpectedly.

HANG UP.

You are allowed to end the call. You do not have to stay on the telephone because the caller sounds official, friendly, worried, or urgent.

DON'T CLICK.

Do not click links or open attachments in an unexpected email or text. A message can look professional, contain a familiar logo, and still be fraudulent.

CHECK.

Contact the person, bank, business, government agency, or family member yourself using a phone number or website you already trust. Or talk to someone on the Otwarte Circle team before doing anything.

Warning signs that should make you stop

- Someone tells you to act immediately.
- Someone tells you not to tell your family, your bank, or anyone else.
- Someone asks you to move money to “protect” it.
- Someone asks for a gift card, cryptocurrency, wire transfer, cash, or precious metals.
- Someone asks for a password or one-time security code.
- Someone wants remote access to your computer or phone.
- An email or text asks you to click a link to fix an urgent problem.



- A caller threatens arrest, legal action, loss of benefits, or another frightening consequence if you hang up.
- A family member suddenly needs money and asks you to keep it secret.

Caller ID and email addresses can be faked

Seeing a familiar name or telephone number on your screen does not prove the call is genuine. Scammers can spoof caller ID. They can also create email addresses, websites, logos, documents, voices, and even videos that look or sound convincing.

That is why the safest response is not to judge the message by how professional it looks. Verify it independently.

What if you already clicked, answered, or gave information?

Please tell someone right away. There is no reason to be embarrassed. These scams are intentionally designed to create fear, trust, urgency, or confusion.

If money or banking information was involved, contact your financial institution immediately. If a password was shared, change it promptly and use multi-factor authentication when available. If you clicked a suspicious link or allowed access to a device, stop communicating with the caller and get trusted technical help.

You can also report fraud to the Federal Trade Commission at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud) and internet-enabled crime to the FBI at [IC3.gov](https://www.ic3.gov). Suspicious texts can be forwarded to 7726 (SPAM).

One last time

If an unexpected call, email, or text asks you for money, personal information, a password, a security code, or immediate action:

STOP. HANG UP. DON'T CLICK. CHECK.

And if you are uncertain, talk to someone on the Otwarte Circle team. We would much rather have you ask us about a legitimate message than have you feel that you needed to figure it out alone.

Thank you.

Cindy, Nonah, and Teran