Protect Yourself From Scams

How do scammers work?

They may pretend to be someone they are not (such as a family member, a government official, a tech support person) and reach out to you via text, email, or phone call. Common goals of scams include:

- Installing malicious software onto your device
- Getting you to pay money to them
- Obtaining key information about you (e.g., credit card numbers, SSN, and passwords)

How do I know if something might be a scam?

Ask yourself:

- Is this an unsolicited phone call, text, or email?
- Does the message appear unusual for the sender/caller?
- Is the message vague about who it is addressed to or key details?
- Does the message convey urgency (e.g. “must act now”, “offer ends soon”)?
- Does the message seem too good to be true?

Verify the message:

- Search online. Did other people report this message as a scam?
- Contact the sender through another channel (e.g., if they claim to work at your bank, call your bank’s official number).

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

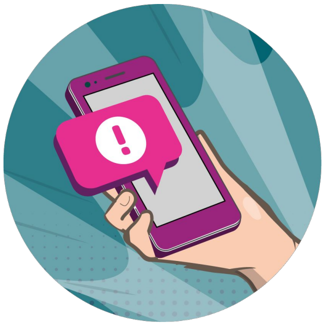
Protect Yourself From Scams

I fell for a scam! What do I do now?

If the scammer gets your password, **change your password immediately.**

Enable two-factor authentication if your service allows it, so that you can stop a hacker even if they have your password.

Alert your bank of the situation. Get a new credit card number and freeze your existing card. Keep a close eye on your statements and report any fraudulent charges.



Report the scam to your service provider, the local police, and to the federal government, so that others don't receive it.

More info on how to report scams: https://www.usa.gov/stop-scams-frauds