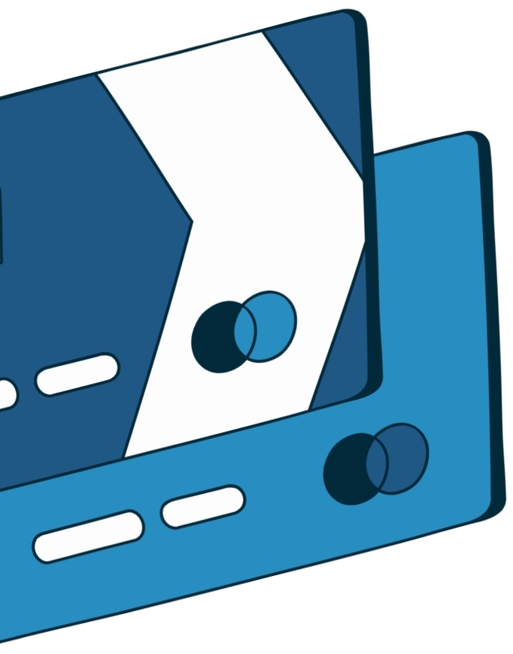
Ways to Protect Yourself from Fraud

The power is in your hands. Here are some common examples of fraud and how to keep your information safe.



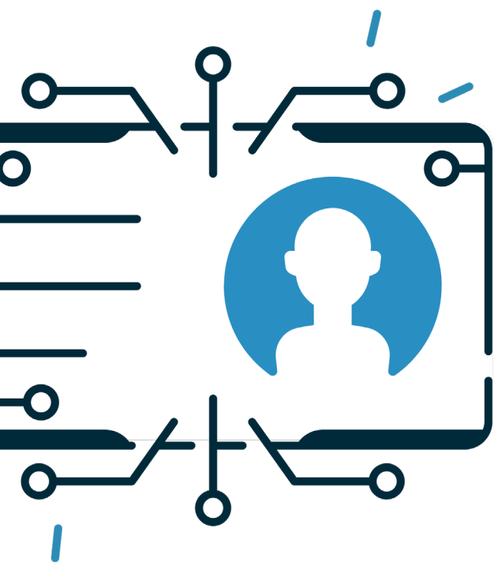
Unauthorized Withdrawals

What It Looks Like:

A fraudster gains access to your account number, possibly by stealing or finding discarded bank statements, and makes withdrawals from your account without your permission.

How to Protect Yourself:

Make sure you're keeping account numbers safe and shredding financial documents.



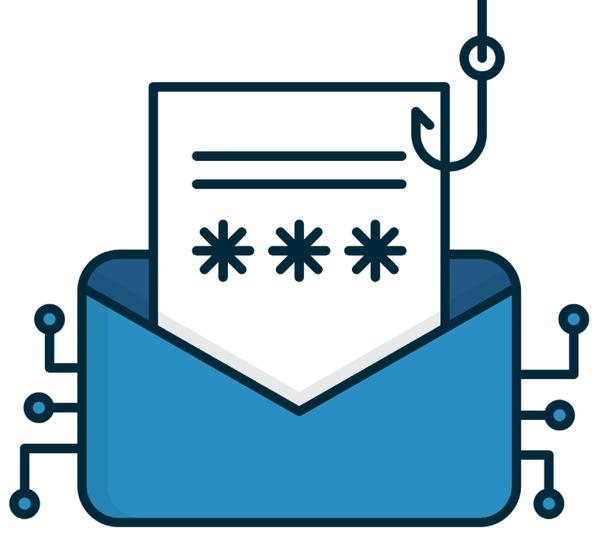
Identity Theft

What It Looks Like:

Someone uses your personal information, like your Social Security number, to gain access to a credit card number or bank account number. The fraudster uses this information to make unauthorized purchases or withdrawals, open new credit cards, take out loans or commit other types of fraud in your name.

How to Protect Yourself:

Notify credit reporting agencies and account opening agencies, such as Chexsystems, if you are a victim of identity theft.



Phishing Schemes

What It Looks Like:

You receive an email, unsolicited QR code, text or phone call pretending to be from a trusted source, asking you to "verify" your account information by clicking a link or providing sensitive details.

How to Protect Yourself:

Don't click on unsolicited emails, texts or links, and avoid using public Wi-Fi. Look for red flags, like a request to verify or unlock your account, urgent language, or grammatical errors. ESL will not ask you for personal information, such as your passwords or full SSN. Ensure your computer and devices are protected by software or multi-factor authentication.

Extra Tips to Help You Safeguard Your Information

- Don't use unfamiliar websites to download free stuff, like music or movies.
- Don't download content through peer-to-peer file-sharing sites.
- Don't rush to make payments to merchants that threaten or request urgency. Also, stay wary of correspondence that asks you to refrain from saying anything to your financial institution.

Fraud Happens. What's Next?

1. If an imposter "phishes" information from you: Block and report the numbers you're being called from and contact ESL immediately.
2. If your card is compromised: Review your statement and report issues — the sooner you report, the sooner we can work to help you resolve it.
3. To report scammers to the Federal Trade Commission (FTC), go to ReportFraud.ftc.gov.
4. Email us at **Fraud_Prevention@esl.org** if you're unsure or have any questions.
5. Call us at **585.336.1000** if you think your account may be at risk.

You've got this!