Protect What's Yours

Stay One Step Ahead of Fraud with ESL

Staying informed is your best defense against fraud. By taking proactive steps, you can safeguard your information, secure your accounts and stay one step ahead of potential threats.

Fraud Question & Answer

What is **phishing?**

Phishing is when someone tries to trick you into sharing personal information – like your passwords or banking details – by pretending to be a trustworthy source. Phishing scams often convey a sense of urgency to try and urge you to act fast.

How can I keep my information **safe from phishing schemes?**

Take your time and carefully review the message – don't let fraudsters rush you into making a rash decision. Check for consistency in the message, independently verify the legitimacy of URLs, refrain from sharing one-time use passcodes, and never give away personal information via unsolicited text messages or phone calls. It's also important to remember you should never click on links or log into your account through a suspicious text message or email. When in doubt, exercise caution and don't engage with the message!

How do I protect my personal and financial information while **shopping online?**

To safeguard your information, shop only on secure, trusted websites. Always enable multi-factor authentication on your accounts, avoid using public Wi-Fi for transactions and regularly check your accounts for unauthorized activity.

How can I **protect my accounts** from fraud?

Use strong, unique passwords, enable multi-factor authentication, set up security alerts and adopt proactive habits like regularly reviewing your accounts. You can also stay informed through our educational resources on esl.org. These steps will help you manage risks and stay ahead of evolving fraud threats.

How can I stay safe while using **ATMs and drive-up teller services?**

Never deposit a check into your account for a stranger. Fraudsters may persuade you to assist by offering you a portion of their deposit. Do not be their associate. If you see suspicious activity at an ATM or drive up, contact local law enforcement authorities immediately. Otherwise, we recommend staying aware of your surroundings at all times, using ATMs that are well-lighted, covering your hand when entering your PIN at an ATM and monitoring your accounts daily for suspicious transactions.

What resources are available to help ESL members **proactively prevent fraud?**

At ESL, we use advanced encryption methods and monitor accounts for suspicious activity 24/7. We also offer the capability for members to set up text and email alerts for withdrawals, deposits, balance updates and more. Members may also find a variety of educational resources on esl.org designed to help you protect your information from fraud.

Our team is here to help.

Concerns? If you think your account is at risk, call us at

585.336.1000

Questions? Email us at

Fraud_Prevention@esl.org