Safeguard Your Business Against Fraud with ESL

When you're informed, you're empowered.

Stay one step ahead of fraudsters and schemes. Here are some questions you might have throughout your day along with the answers you need — so you can feel confident and secure at work.

Fraud Question & Answer

What is **phishing?**

Phishing is when someone tries to trick you into sharing your organization's information – such as your login details or security questions – by pretending to be a trustworthy source. Fraudsters often target businesses by posing as financial institutions and law enforcement. To do so, fraudsters often target businesses by disguising their phone call, text, or email to appear as the trusted organization. For example, fraudsters may call you from a phone number that looks identical to your financial institution's phone number.

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

Never share sensitive information, such as your login credentials or the answers to your security questions, via a phone call, text message, letter, or email you have received. It's also important to remain diligent against invalid email addresses, suspicious links and time-sensitive requests urging you to share account login information. Of note, fraudsters often leverage phishing emails to pose as a trusted vendor. Exercise caution and refrain from sending payments to fraudulent emails. When in doubt, don't engage with the email and call the vendor directly through your usual communication method.

Can my **employees play a role in safeguarding our information?**

Absolutely! Fighting fraud is a team sport. It's important to educate your employees by providing consistent cybersecurity training, equipping them with the information they need to stay diligent against phishing emails, and up-to-date fraud prevention resources. That way, they'll help you safeguard your business, day in and day out – because building awareness never stops.

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

- Regularly review your accounts for any unusual activity
- Use strong passwords and update them frequently
- Assign user access only when necessary
- Keep security tools and associated signatures up to date
- Use caution when connecting to public Wi-Fi
- Establish fraud prevention practices
- Utilize bank security products such as Positive Pay and UPIC

How can I **enhance my organization's fraud controls?**

- Go paperless
- Keep business and personal accounts separate
- Conduct background checks on employees who will have access to sensitive business accounts
- Monitor company cards and spending activity
- Avoid providing confidential information over the phone, through email or via the internet unless you're certain you are doing so securely

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