Sound Business Practices

Good business practices in preventing Corporate Account Takeover include:

- Utilizing dual control for all online transactions.
- Using and keeping all anti-virus and malware detection and prevention software up to date.
- Restricting online banking access to within business networks and firewalls. Avoiding public networks.
- Minimizing computer use where online banking is performed. Do not use this computer for general online navigation and avoid social networks. Employ "safe browsing" software that prevents malware and key-logging software from running.
- Monitoring and reconciling your accounts daily and being diligent in detecting anomalies.
- Using the alerts provided by Lincoln Savings Bank's online banking system to notify of transaction creation.
- Utilizing out-of-band authentication (the use of two separate networks working simultaneously to authenticate a user) at login and also at transaction creation.
- Keeping account limits as close to business needs as possible.
- Utilizing additional fraud prevention services like Positive Pay (a provided service that matches checks a company issues with those that are presented for payment) and ACH block to pro-actively prevent fraud.

Fraud and Phishing

Phishing scams are typically fraudulent e-mails or messages that appear to come from legitimate sources. The e-mails may contain malware as discussed in the "Corporate Account Takeover" section, or may contain links to impersonated websites (phishing). The phony website appears to be a website that you may otherwise use in all facets. However, when entering login credentials, it will generally present a page that indicates the site is down or unavailable. However, fraudsters have already logged your credentials to the real site and can begin attempting access. It is important to stay diligent in monitoring these types of e-mails to help protect against unintentionally exposing securing data. Some of the things you can look for are:

Unauthenticated E-mail Addresses

Because e-mail addresses can be spoofed, you need to authenticate the legitimacy of the sender. Some Internet service providers have stronger filters than others and will check the sending IP against an authenticated IP address and domain name server.

Typos and Grammatical Mistakes

Fraudulent e-mails are often mass generated and even translated using software from foreign languages and contain nonsensical grammatical flows, incorrect syntax, or use of pronouns. It is also common place to intentionally use incorrect spelling to bypass industry standard spam filters.

Awkward Greetings

Generic greetings that are not referring directly to the recipient. May be generally stated such as "Client:"

Sense of Urgency

Many phishing e-mails use compelling language for an immediate call to action. They will encourage you to act immediately for the sake of security or to prevent fraud/loss.

Randomly Generated Numbers

Phishing e-mails may seem to have included account numbers or reference numbers to try and add "legitimacy" to their message.

Links

Be cautious of links. Many phishing e-mails rely on external links to direct you to a spoofed website where they will gather information you willfully enter. Some phishing websites are blatant enough to ask you to enter account numbers, debit/credit card numbers, security codes, and PINs. By hovering over the link in an e-mail, you can occasionally view the source code to where the link is directed and this may be an obvious indicator.

Use of Logos, Websites, and Addresses

In an attempt to seem legitimate, phishing e-mails may contain authentic business logos, addresses and phone numbers to help lower your initial skepticism of the e-mail.