Butwin Insurance Group
Founded 1925

Understanding the Risks of Deceptive Funds Transfers, Social Engineering and Cyber Crime

"Phishing" Schemes Can Make You Fall for It "Hook, Line and Sinker."

You or someone in your company has received an e-mail which appears to be from an executive of the firm instructing you to wire funds to a specified address.

You receive an e-mail or phone call which appears to be from a vendor instructing you to change its banking information.

Social engineering (also referred to as "phishing") is a term the defines the manipulation of humans into performing acts or divulging confidential information. It's not a new concept. In fact, everyday more and more small- to medium-sized businesses fall victim.

A social engineer is nothing more than a con man who uses technology to swindle people and manipulate them into disclosing passwords or bank information or granting access to their computer. Understanding how these social engineers work and the schemes they employ is key to implementing successful internal controls which minimize the risk of significant loss.

Watch Out for These Potential Scenarios for Deceptive-funds Transfers:

1. A fraudster, through emails, telephone calls or both, poses as a company executive, vendor or customer, and convinces an employee to transfer funds
2. The hack and transfer are enabled by employee negligence
3. The financial transfer is effected entirely by a hacker independently penetrating a computer system, and making the transfer themselves
4. A fraudster convinces an employee to reveal their credentials, then enters the network by using them, and ultimately transfers funds
5. A fraudster entices an employee to open an attachment or click on a link, thereby allowing the network to be penetrated, and facilitating the transfer of funds
6. An employee enters data believed to be accurate which is, in fact, fraudulent
7. A rogue employee makes an improper transfer or enters fraudulent data

Common Forms of Phishing:

Deceptive Phishing:
Email messages claiming to be from recognized sources ask you to verify or re-enter info, or make a payment.

Spear Phishing:
Sender uses available info to direct their request at you.

CEO Fraud:
Use an email address of a principal or senior manager to request payments of information.

Pharming:
Hijack your domain and redirect to an imposter site.

Dropbox Phishing:
Realistic-looking emails requesting user to "secure" their account or download documents.

Google Docs Phishing:
Invites access to Google Docs and entering credentials into the hands of scammers.

Often Insurance is Not the Best Risk Management Solution. We Recommend That Everyone Implement Loss Control Procedures and Training.

The growing use of technology-enabled fraud is evolving faster than the courts or insurance carriers can react. From an insurance perspective, crime policies were designed to cover an employee stealing from the firm. Cyber Insurance was designed (in addition to other exposures) to protect against an outsider hacking into your computers. **Neither of these policy types were designed to cover an employee's conscious decision to intentionally release information or funds, even if induced through fraud or deceit.**

Insurance carriers have just recently started to roll out coverages to protect against these exposures. However, there are still issues that remain:

- The carriers themselves are not sure what all the exposures are and how to properly cover them.
- The coverages being offered are completely different from carrier to carrier – and are all very limited on their own and compared to each other.
- The exposures are spread out over: messages from trustworthy sources, phishing schemes, baiting scenarios, impersonating superiors, compute fraud and funds transfer fraud. There is no one product to protect against all of these exposures and no sure and tested group of products to fully protect against this wide range of exposures.
- Due to the newness of this fraudulent activity, courts have not yet established which coverages are actually responsible to respond to these losses.

Butwin Insurance Group cares deeply for the success and financial well-being of your business and offers comprehensive insurance solutions to proactively protect you professionally and personally. In this case, however, insurance is not the best risk management solution. We strongly recommend you implement the following loss control procedures and training:

- **NEVER** add new or edit existing wire transfer instructions without making an outgoing phone call confirming the instructions are from the requestor.
- **NEVER** open an attachment, download a file, provide or confirm information, etc. from any person via an e-mail even if you recognize their name. First hit "REPLY" and CAREFULLY CONFIRM that the e-mail address showing in the reply e-mail address confirms WITHOUT A DOUBT that this is the person they say they are. In many cases the email address appears to be the same, however, one letter may be changed.

60 Cutter Mill Road, Suite 414
Great Neck NY, 11021
(516) 466-4200
www.butwin.com
info@butwin.com