Need Assistance?
bigimarkets@iiaba.net
703-647-7800 (9am-5pm ET)

Engineering a Social Fraud

Remember the "Nigerian prince" email scam? I don't know how many people fell for it over the years, but it was successful enough for it to exist for decades. This is an example of a social engineering fraud.

There are two main types of social engineering frauds. Mass frauds are usually simple and involve a large number of potential victims. Targeted frauds are more sophisticated and are directed at very specific individuals or companies.

While the scams themselves differ, the methods used by criminals generally follow the same four steps:

1. Gathering information
2. Develop relationship
3. Exploiting identified vulnerabilities
4. Execution

Most scams go after individual people or families, but businesses are not immune.

Email scams/hacking of email accounts/manager fraud
Fraudsters gather publicly available information - usually through the Internet - about the company to be targeted, specifically the managers and employees who are authorized to handle cash transfers and use this to impersonate the higher-ups and trick employees into making a high-value cash transfer to a designated bank account. There is usually a element of urgency involved so the employee is more likely to skip certain security protocols. In 2015 the FBI issued a PSA about the increase of this type of scam.

Other techniques include:

- Retrieving unsecured materials (USB keys, hard drives) from the trash;
- Quid pro quo - Exchange of sensitive information under a misunderstanding;
- Baiting - Leaving an infected storage device to be picked up and plugged into a computer;
- Tailgating - Following someone to access secured premises;
- Diversion theft - Redirecting a courier or transport delivery to another location.

Travelers offers a **Social Engineering Fraud Endorsement** that can protect your clients' assets against what can be complex and unique perils. Among other information the linked flyer includes three examples of social engineering frauds.

Fidelity/Crime from Travelers covers employers for direct loss as well identity fraud reimbursement and reasonable claim expenses. Travelers has also put together a quick (under two minutes!) video to help explain it. Watch "Fidelity and Crime - Demystify Management Liability" now and feel free to share this with your clients.

Fidelity Crime can be obtained singly or as part of **Wrap+ for Executive Liability for Private Companies**. You can pick

Original Article Publication Date – February 20, 2018

and choose the coverages your client needs and leave off what they don't. In the future you can add new or drop old coverage as needed.

Click the links below to learn more about available options, access highlight and sell sheets, and more:

- Directors and Officers Liability Insurance
- Employment Practices Liability Insurance
- Fiduciary Liability Insurance
- Miscellaneous Professional Liability (E&O) Insurance
- Crime Insurance
- CyberRisk
- Kidnap and Ransom
- Identity Fraud Expense Reimbursement

As part of the coverage, your clients receive access to *Risk Management Plus+ Online*[7reg;], a one-stop resource that provides a comprehensive set of tools to help protect their organization from costly litigation. To learn more, visit www.rmplusonline.com.

To access the Wrap+ please log into Big "I" Markets and look for Wrap+ products in the commercial product listing. Please note that the Community Homeowners Associations and Healthcare Organization are not currently available through Big "I" Markets.