NORTHERN TRUST

PROTECT YOUR BUSINESS FROM SOCIAL ENGINEERING

April 2018

SECURITY PRECAUTIONS

Many companies keep sensitive personal information about customers or employees in their files. Having a sound security plan in place to protect this information is crucial, and an important part of any plan is educating employees about the threat of social engineering.

Educate your employees about the importance of good security practices. Displaying company identification badges, preventing the practice of Tail Gating (a.k.a. "Piggybacking"), and taking care to keep conversations about company business private are all good security practices.

WHAT IS SOCIAL ENGINEERING?

In its simplest form, Social Engineering is the act of manipulating people into performing actions or divulging confidential information.

HOW DOES SOCIAL ENGINEERING WORK?

Social Engineers typically use any means available to get the information they want — information that can then be used to perpetrate Identity Theft, commit fraud, or be exploited for other illicit purposes.

WHAT CAN YOU DO TO PROTECT YOUR BUSINESS?

Stop Social Engineers by following a few these important security precautions, including: ■

- **Lock it up!** Computer defenses can be critical, but when it comes to protecting personal information, don't forget basic physical security. Make sure every employee has a secure drawer or locker. Limit access to information to those employees with a legitimate business need. Enforce a clear desk policy — encourage employees to lock up documents when they are away from their desks and consider encrypting data before shipping it offsite.
- **Keep up your defenses.** Viruses, spyware, and other invaders are a constant concern for an unprotected computer. Technology controls won't help without some help from your users — strong passwords that are properly

protected are essential. Keep your systems patched and ensure your security controls are appropriate for your organization.

- **Educate your employees.** Although hackers certainly pose a threat, sometimes the biggest risk to a company's security is an otherwise conscientious employee who hasn't learned the basics about protecting personal information. Create a culture of security by making it clear to staff that abiding by your company's data security plan is a critical part of their job. Make account data, credit card numbers, or other sensitive information available only on a "need-to-know" basis.■
- **Trust, but verify.** Before outsourcing any of your business functions — payroll, web hosting, data processing, fulfillment, and the like — investigate the company's data security practices and compare their standards to your own. Make sure your requirements are spelled out in the contract and built in a way for you to monitor their performance. Insist that service providers notify you immediately if they experience a security incident, even ones that do not compromise your data.