10 Best Practices for Online Security and Fraud Protection

- Types of Fraud ... and Fraudsters
- 10 Best Practices for Combating Online Fraud
Types of Fraud ... and Fraudsters

As more commerce goes online, among the hottest of hot-button issues for today's businesses is security. Online transactions have become increasingly prone to the risk of cyber-threats, in the form of malware, fraud and unauthorized access to accounts.

Cyberspace can be a dangerous environment, and is becoming more so. Recently, hacking has evolved at a troublingly fast pace. Today’s perpetrators are not only more sophisticated, but they are also more likely to be professionals. The conventional profile of a fraudster — a young hacker sitting at his laptop, violating company records for the fun of it — has become rather outdated, even quaint. Online fraud today is a formal, large-scale and highly lucrative criminal enterprise, with multiple parties collaborating to perpetrate fraud against clients. It is an industry-wide problem.

There is not just one type of fraudster. They come in at least three flavors:

- **Joy riders (people with a cause).** These are the wiki-leakers and other individual hackers, anonymous and otherwise, about whom one typically reads in the news. They generally target large, public companies. In short, it’s not financial information they’re after; it’s embarrassing corporate dirty laundry.

- **IP seekers.** Their goal is to confiscate information about a business, its dealings, its client roster, etc. They may sell this information to competitors. Or they may defraud the company’s clients — or even the clients’ clients — with ersatz emails and the like.

- **Hunters of easy prey.** A large and growing contingent, these fraudsters target banks’ clients: small and midsize companies that are less likely to have and spend capital on building a robust IT security infrastructure. Their motivation is pure financial gain.

One characteristic that marks all of the above fraudsters is patience. They do not strike indiscriminately. Rather, they are diligent, biding their time, conducting extensive research into the companies they target. They even employ developers to write malware for them.

Even CFOs, treasury officers and other finance professionals who are aware of the risks inherent in online transactions can benefit from guidance on preventing online financial fraud. Following are 10 best practices that companies can employ to help mitigate their risks.
1. **Apply offline diligence to online behavior**
   Begin with the same diligence that business people have used to prevent offline fraud for decades. For example, requiring a senior executive’s countersignature on payments of over $10,000 is a de facto requirement for paper checks. That requirement often goes by the wayside, however, when applied to online payments. Dual approval should be required for all high value wires or automated clearinghouse (ACH) transfers.

2. **Institute strict online payment rules**
   In addition to dual approval, companies can establish other rules regarding online payments.
   - Require PIN entry at initiation and/or approval.
   - Set approval limits at the user level, by template or by transaction type.
   - Enable wire alerts to notify users of pending exception items.

3. **Install layered security software**
   Besides the anti-virus software installed on all workplace computers, small and midsize companies should install additional security, such as an anti-financial malware tool. Among the best known of the affordable security software programs available is Trusteer (trusteer.com), a powerful, browser-based anti-financial malware tool. More than 100 banks — SunTrust among them — offer this tool to their clients.

4. **Assign an online banking computer**
   Designate specific computer(s) exclusively for online banking. Avoid conducting online banking business activities on home computers or at publicly shared (WiFi) locations such as hotels, airports and coffee shops.

5. **Protect your ACH transactions**
   Many fraud attempts are focused on violating ACH transactions. Here are some preventive measures:
   - Prenote zero-dollar transactions to verify the recipient routing number and account number before sending a live-dollar transaction.
Many fraudsters have discovered that it is easier to be invited in to a company than to try to infiltrate it, devising clever ways to disguise themselves as trusted online service providers.

6. Secure your wire transfers

Wire transfers are as susceptible to hacking as ACH transactions. You can take these steps to help keep them secure:

- Use bank-defined wire templates to reduce the risk of unauthorized changes to beneficiary routing information.
- Call in international wires directly to the bank if you use them infrequently.
- Ensure that user limits are established on your wire transfer system.

7. Restrict personal activities

Employees’ personal email accounts and personal web surfing are notorious security soft spots. It is important to restrict staff use of personal email accounts and websites on company computers.

If you wish to be less restrictive, simply require that employees exercise caution when going online. A few tips:

- Distinguish between “safe” online practices — making an Amazon.com purchase — and “unsafe” practices, such as visiting an unknown blog or friending an unfamiliar Facebook contact.
- Do not click on links or respond to requests for information in unsolicited emails.
- Report any suspicion of viruses or computer performance issues to the appropriate authority at the company.
8. **Beware of email dirty tricks (i.e. “phishing”)**
   A prevalent ploy: emails that trick a company’s personnel into installing malware on their PCs. This malware is then used to steal passwords and User IDs to commit wire and ACH fraud. This is known as “phishing.”
   Even senior executives have been duped by authentic-looking emails, such as the now-infamous “UPS shipment notice” that automatically downloads malware when opened. It is a perfect illustration of computer security specialist Bruce Schneier’s famous quote: “Amateurs attack machines; professionals target people.”

9. **Manage security updates**
   Make sure all employee computers have the most recent security patches. It’s easy to install updates, since PC operating systems generally support these downloads. Simply make sure the “allow updates” setting is turned on. Once activated, security patches can be downloaded at regular intervals. Of course, you should always be sure to review each update before installing it.

10. **Maintain code confidentiality**
    Protect your users’ authorization passwords by:
    - Creating alphanumeric passwords that are difficult for others to guess.
    - Using difficult-to-guess security challenge questions and answers.
    - Never sharing passwords, wire PINs, or account information.

SunTrust is committed to helping small and midsize companies keep their online transactions safe from fraud. By implementing these security best practices, you can help mitigate the risk of unauthorized access. For further insight and a discussion of your online financial security needs, please call your SunTrust Relationship Manager or Treasury Sales Officer.