Simple precautions reduce risk of online financial fraud

The Internet has truly changed the way business owners conduct their daily operations. In an instant, and from any location, you can pay bills, notify customers of special promotions, monitor account activity, deposit checks, catch up on financial news and communicate with suppliers. As commerce continues to become more Internet-based, so does the nature of financial crimes against North Texas businesses.

Bryan Thomas
Guest column

Whether you are a large corporation or a small family enterprise, all companies share a similar risk of being targeted by fraudsters and hackers. Since the best defense is a good offense, the more you can do to assure safe and sound banking practices for your business, the more your security is increased.

Many business owners do not have adequate security measures in place because they do not fully understand the various ways these fraudsters work. One of the most common forms of attack is by hacking in and infiltrating company computers (and sometimes personal computers used for company purposes) to install malware and viruses that capture the login, password and, in some cases, the dynamic security token number information of a legitimate user. Fraudsters are also launching "man-in-the-middle" or "man-in-the-browser" attacks to capture online banking log-in information by asking a customer to reenter log-in information or to answer additional challenge questions. Capturing such information allows the fraudster to login to your company's online banking system and impersonate a legitimate company user, enabling them to transfer funds, typically by wire or Automated Clearing House (ACH) transfer, to accounts in other banks inside or outside the U.S.

Another form of attack enables fraudsters to obtain all of your company's online banking information, and then transfer the money by wire or ACH into the personal accounts of often-unwitting "electronic money mules." These are people who have been previously recruited via Internet job posting sites for positions that include, among other seemingly legitimate job duties, processing payments to foreign entities out of their personal bank accounts. Hackers fraudulently transfer money from a company's account to the personal account of the electronic money mule. Once the funds are deposited, hackers instruct the mule to immediately withdraw the funds in cash and send them via Western Union, MoneyGram or another international remittance company to an account located outside of the country.

The fraudsters in these situations move quickly, and the key to fighting this type of crime is to proactively strengthen internal online banking procedures before becoming the victim of such an attack. Some of these procedures could include:

• Monitor your accounts frequently and immediately report any suspicious activity to your bank.

Whether you are a large corporation or a small family enterprise, all companies share a similar risk of being targeted by fraudsters and hackers.

• Limit the number of and type of employees who can originate transactions, and keep your computer systems up-to-date and protected.

• Never share user IDs, passwords, PINs (Personal Identification Numbers), dynamic tokens, etc., with anyone, and do not leave any such information or items in an area that is not locked or secured.

• Obtain and install a firewall, antivirus, anti-malware and anti-spyware software. Make sure these protections are active and automatically updated by your vendor (or take necessary steps to keep them updated).

• Limit or eliminate unnecessary web surfing and e-mail activity, including personal activity, on computers used for online banking.

• Educate all personnel on good cyber security practices, including clearing the Internet browser's cache before visiting the financial institution's Web site and knowing how to avoid having malware installed on a computer.

• Never leave a computer unattended when using any online banking or financial services, and never conduct online banking from a public computer.

*Do not click on a link in any e-mail purported to be sent from a bank. The bank's official e-mails will always instruct you to log into online banking for updates, instructions, notifications, account statements, etc.

• Be suspicious of e-mails purporting to be from other financial institutions, federal, state or local government departments or agencies, or taxing authorities that request personal information. Remember, important communications such as legal process, subpoenas and other information from government agencies will still generally be delivered as regular snail-mail.

No matter how secure your business computers may be, every owner has a responsibility to protect sensitive information and accounts from unauthorized access. Although you cannot completely eliminate the risk of being impacted by a fraud incident, implementing these common sense measures will make it more difficult for fraudsters to carry out their schemes and encourage them to move along to another victim. ■

Bryan Thomas is senior vice president of the Treasury Management department at OmniAmerican Bank. For information, visit www.OmniAmerican.com.

▶READING from page 10

two pieces then four," Taylor said.

One of the more popular hands-on projects, Taylor said, is delivered before the children's eyes – literally.

"We order chick eggs and the children can watch them hatch," Taylor said. "It's one of their favorite sections of science when UPS delivers the eggs and we tell them '21 days from now these are going to be chicks.'"

To date, Taylor said she has a yard full of chickens residing at her home.

For all of the similarities, though, there also are many differences between the schools. Most of the Reading Friends schools, for example, offer four-hour days and kindergarten classes, but the Fort Worth school operates only three hours per day and does not offer kindergarten classes.

"Most of our children are going to private schools and private schools want to get them in kindergarten," Spencer said. "It's important that each school offers what its parents need."

Summer classes also differ. Taylor offers classes in June and in August while some other franchises offer summer classes on a much different schedule. Taylor said her parents typically go on vacation in July so she changed her summer course offerings to accommodate.

One of the biggest differences, however, comes in pricing. Spencer said the Fort Worth school runs between $300 and $500 per week depending on the class, while Taylor's Aledo school averages between $275 and $450 per month, with kindergarten classes running $495 per month

Spencer said there is a waiting list of about 30 children on any given class list annually, but the waiting system is a great improvement over her early system.

"Parents used to camp out," Spencer said. "We used to have pre-registration day and people would line up and camp out overnight, but we did away with that about 10 years ago."

Spencer said these days, it's not uncommon for her school to receive calls regularly from hospitals from parents wanting to put their newborn on the waiting list. Even so, Spencer said some years her school is able to work through the waiting list so parents are always encouraged to add their child's name to the list.

"It's a niche in the community that fills a need and we feel extremely blessed," Spencer said about the success of Reading Friends, which graduates about 144 children per year.

"I didn't realize it, obviously, but now I know I have dedicated my life to the young child and all the possibilities therein and those possibilities are just endless. I learn something all the time. I'm amazed and I think 'why didn't I figure that out 30 years ago?'"

Spencer said she hopes to continue to grow the school franchise, and she looks to cities like Dallas, Arlington and Mansfield as possible opportunities.

"The best location is an area with a high concentration of mobile, young families, but we are certainly open," she said. "We just want to reach more and more families, but in a small environment. That's how it started and that's how it will continue because when you get too big you lose that personal contact and for young children, that's never good." ■