IT - PASSWORDS, THE INTERNET & LAPTOPS

by Steve Brown

Yesterday, we locked in on things community bankers can do to protect sensitive data. Today, we discuss a few more technology tips worthy of knowing. While many community banks are already doing an excellent job at protecting information, there is always more that can be done. With that in mind, here are some additional things we think community bankers will find interesting.

Passwords - studies find 61% of people use the same password for everything, 50% base them on the name of a family member, partner or a pet, 30% use a pop idol or sporting hero. In short, people are horrible at creating passwords. As humans, we inherently try to make passwords simple so we can remember them. The problem is that doing this also makes it easier on the bad guys. As some guidance, try these quick tips - avoid using words in the dictionary; insert numbers or special characters between alphabet letters in the password; never share your password with anyone; make your password at least 8 characters (note also that a 15 character password composed of random letters and numbers is 33k times stronger than an 8 character password); ideal passwords combine both length and different types of symbols; add complexity by mixing uppercase and lowercase letters and numbers; don't use your login name; change your password regularly; never email your password and never type your password on a computer you do not control (i.e. in a hotel lobby).

Internet Usage - there are lots of bad guys out there, so bankers need to be careful when employees access the internet. Banks should warn customers and employees alike not to ever give out bank account or credit card information; only deal with known companies; ensure the lock at the bottom of the PC is locked; when exchanging secure information make sure the connection is secure (https); do not open email attachments from those you don't know; be wary of any "known" company that asks for your personal or sensitive information (phishing); maintain a strong firewall and antivirus program; monitor employee activities; provide training to raise awareness of common issues; frequently change passwords (about every month); don't leave your computer online when you are not around (or overnight when you sleep); only connect to trusted sites you know; avoid downloading information from sites you do not know; make sure you get security updates; don't click on a link without considering the risks and knowing the source; check the web page address you have been taken to when searching, to be sure you haven't been moved to an unexpected site.

Laptops - did you know a recent study found 81% of US companies lost laptops with sensitive data during the past year? Employees or management team members that have been assigned laptops must consider the extra burden of security they are literally carrying around. Laptops should never be left unattended; information on them should be encrypted; they should never be placed in checked baggage when traveling; they should not be left in hotel rooms, cars, conference rooms or restaurants; don't use a computer bag to carry the laptop (is an advertisement for theft); keep the serial number in a safe place (in case you need to file a police report); be aware of your surroundings (some thieves are gutsy enough to just run by and grab the laptop); lock the laptop in your office during off-hours and use a cable lock (it will slow crooks down) when traveling.

While technology is fun and productive to use, making sure the bank is protected and data is secure just makes good business sense. Remember that IT security is not the exclusive domain of the IT department, but rather it is a team effort, requiring the participation of every employee.

BANK NEWS

TLGP Extended

The FDIC announced late yesterday that they will extend TLGP through October.

Branch M&A

Bay Commercial Bank ($104mm, CA) has agreed to purchase a branch from Community Banks of Northern California ($193mm, CA) for an undisclosed sum. Community Banks belongs to a $2B 3 bank holding company (Community Bankshares Inc. of CO).

Expected Failures

RBC Capital Markets estimates over the next 3-5Y, more than 1k banks may fail (or 1 in 8 banks).

ARM

ARM applications dropped to 3% of all loans in December as 30Y fixed mortgage rates have dropped to the same if not lower than initial arm rates. During the housing boom ARMs accounted for 36% of all loan applications.

Multifamily Sector

The NAHB is projecting multifamily construction starts will fall to 188k in 2009, from the 350k level more typical over the past few years.

FHLB Exposure

The FHLB system as of 3Q had lent $1T to financial institutions nationwide, up from $641B as of 4Q 2006.

More Advertisement

A study finds 81% of small businesses plan to maintain or increase advertisement spending in 2009.