Protect and survive

Internet banking has soared in popularity over the past few years, but the banking industry must improve security or risk a major loss of public confidence, argues ***David Rowe***

Sadly, malicious activity is a perennial reality throughout human history. Such activity was evident from the earliest days of the internet, but was long associated with counter-cultural geeks showing off their technical prowess. Over the years, however, it has taken on a more ominous complexion. Organised crime and terrorist groups are increasingly prominent sources of such threats. Accompanying this trend has been the growing sophistication of the methods employed.

Despite this, many banks still allow simple passwords of dubious strength to serve as the sole means of security against fraudulent access. Some of the reluctance to strengthen electronic security may be fear of negative customer reaction to increased inconvenience. While such a reaction is likely to occur, I suspect it will be mild compared with the public loss of confidence if there is a major security breach. Herewith are some modest proposals for improvement.

■ **Require stronger passwords.** Common passwords, such as the name of one's spouse, are easily compromised, especially by someone with knowledge of a person's personal details. Insisting on both upper case and lower case letters and at least one number in the middle of the password should be a minimal requirement. Ideally, we should stop talking about passwords and think in terms of security strings. One approach is to use a short representation of a pass sentence. For example: 'My first dog's name was Spot' could become *M1stdnwS*. This is both easy to remember and results in a hard to crack security string.

■ **Only request partial information.** Some UK banks say they will never ask a customer for a full pin number or security string on the phone or on the web. Instead, they request partial inputs in random order on any given occasion. This is intended to foil key logging programs that can be maliciously planted on a user's hard disk to transmit key strokes to the intruder. Often, user names are quite obvious and are immediately followed by a security string. If this information is captured once, the victim's account is compromised, whereas partial information must be captured several times and organised in the right order before the intruder can be sure of gaining access.

■ **Match the user's computer serial number.** People most often access their bank from no more than one or two computers most of the time. The bank should match the user to the computer attempting to gain access. If it is not the user's normal computer, the bank can demand supplementary verification when access is attempted from unusual hardware, such as a terminal in an internet cafe.

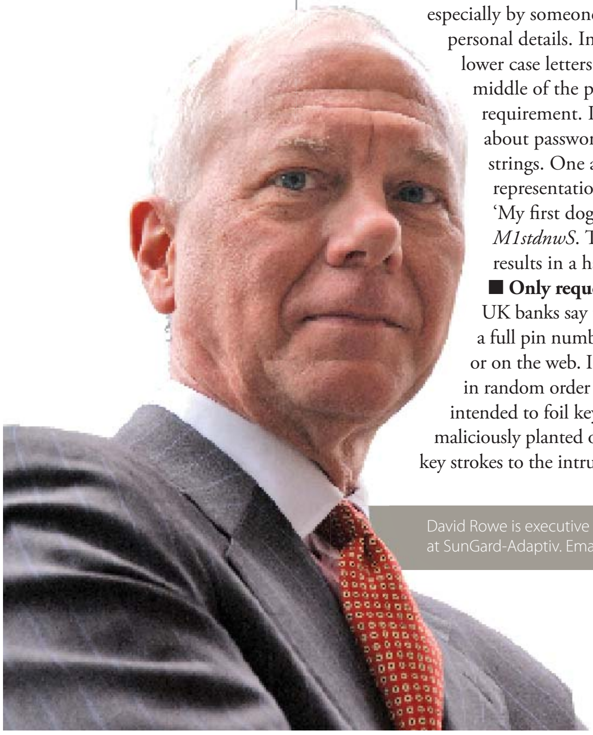
■ **Set up site keys to confirm validity of the bank's website.** Phishing scams attempt to get the user to log into what is supposed to be a bank's website and reconfirm personal details. By setting up a site key system, the user supplies only a login ID on the first screen. The bank website then responds with an image and site key name that have been established by the user. Since a bogus website would not have this information, the user should be alerted to the suspicious nature of the location they have reached.

■ **Two-factor authentication.** Perhaps the most effective improvement in internet banking security would be to implement two-factor authentication for all users. This involves distributing keyring-size tokens that generate a different set of digits every 60 seconds. While these appear to be generated randomly, they are actually created in a predictable sequence known only to the supplier of the token. Users must input both the current digits shown on the token, plus their security string to access their account. Even if someone succeeds in stealing a user's security string, it is useless without also having the token. Likewise, if the token is lost or stolen, it is useless without the user's security string, providing valuable time to notify the bank of the situation.

Even two-factor authentication is not fully foolproof. For example, if users were foolish enough to log into a phishing site and supply their current token digits and security string, the site would have some fraction of a minute to access the user's online account. For this to be effective, such a login would have to be automated because of the short duration for which the token digits are valid. If two factor authentication was combined with a check of the computer serial number by the bank, it would add another layer of security. By demanding further authentication information followed by a request to re-input the token digits and security string, the bank could force enough delay to ensure that the initial set of token digits had expired.

Conclusion

Internet banking is not only tremendously convenient for customers, but is also extremely efficient for banks. By reducing the volume of paper checks and capturing transaction information in electronic form at inception, mistakes are reduced and much of the manual processing is eliminated. If customers are to embrace this mode of banking wholeheartedly, however, they must be confident that it is secure. Many banks have considerable work to do before such confidence becomes a reality. ■



David Rowe is executive vice-president for risk management at SunGard-Adaptiv. Email: david.rowe@risk.sungard.com