Solutions to net security fears

Fake bank e-mails, or phishing, and stories about ID theft are damaging the potential of using the net for online commerce, say e-business experts.

Trust in online security is falling as a result. Almost 70% of those asked in a poll said that net firms are not doing enough to protect people. The survey of more than 1,000 people reported that 43% were not willing to hand over personal information online. It is worrying for shopaholics and firms who want to exploit the net. More people are becoming aware of online security issues but they have little confidence that companies are doing enough to counter the threats, said security firm RSA, which carried out the poll. An estimated 12 million Britons now use the net as a way of managing their financial affairs. Security experts say that scare stories and the vulnerabilities dogging e-commerce and e-banking are being taken seriously - by banks in particular.

"I don't think the threat is overplayed," Barry Beal, global security manager for Capgemini, told the BBC News website. He added: "The challenge for banks is to provide the customer with something that improves security but balances that with usability." Ensuring extra security measures are in place protects them too, as well as the individual, and it is up to both parties to make sure they do what is necessary to prevent fraud, he said. "Card issuers will keep us informed of types of attacks and what procedure to take to protect ourselves. If we do that, they will indemnify us," he said. Many believe using login details like usernames and passwords are simply not good enough anymore though. One of the biggest challenges to improving security online is how to authenticate an individual's identity. Several security companies have developed methods which complement or replace passwords, which are easily compromised and easy to forget. Last year, a street survey found that more than 70% of people would reveal their password for a bar of chocolate.

On average, people have to remember four different passwords. Some resort to using the same one for all their online accounts. Those who use several passwords often write them down and hide them in a desk or in a document on their computer. In a separate survey by RSA, 80% said they were fed up with passwords and would like a better way to login to work computer systems. For many, the ideal is a single online identity that can be validated once with a series of passwords and questions, or some biometric measurement like a fingerprint or iris scan with a token like a smartcard.

Activcard is just one of the many companies, like RSA Security, which has been trying to come up with just that. RSA has a deal with internet provider AOL that lets people pay monthly for a one-time passcode generation service. Users get a physical token which automatically generates a code which stays active for 60 seconds. Many companies use a token-based method already for employees to access networks securely already. Activcard's method is more complex. It is currently trailing its one-time passcode generation technology with UK banks. Steve Ash, from Activcard, told the BBC News website there are two parts to the process of identification. The most difficult is to ascertain whether an individual is who they say they are when they are online.

"The end solution is to provide a method where you combine something the user knows with something they have and present those both." The method it has developed makes use of the chip embedded in bank cards and a special card reader which can generate unique codes that are active for a specified amount of time. This can be adjusted at any time and can be active for as little as 30 seconds before it changes. It combines that with usual usernames and passwords, as well as other security questions. "You take the card, put it in the reader, enter your pin number, and a code is given. "If you wanted then to transfer funds, for instance, you would have to have the code to authorise the transaction." The clever bit happens back at the bank's secure servers. The code is validated by the bank's systems, matching the information they expect with the customer's unique

key. "Each individual gets a key which is unique to them. It is a 2048-bit long number that is virtually impossible to crack," said Mr Ash. It means that in a typical security attack, explains Mr Ash, even if password information is captured by a scammer using keystroke software or just through spoof websites, they need the passcode. "By the time they go back [to use the information], the code has expired, so they can't prove who they are," according to Mr Ash. In the next few years, Mr Ash predicts that this kind of method will be commonplace before we see biometric authentication that is acceptable for widespread use. "PCs will have readers built into them, the cost of readers will be very cheap, and more people will have the cards." The gadgets we carry around, like personal digital assistants (PDAs) and mobiles, could also have integrated card reader technology in them. "The PDA or phone method is a possible alternative as people are always carrying phones around," he said.