Threats to online banking security may alter payment choice

November 16, 2009

During the last several months, a variety of government agencies, industry organizations, and the media have alerted banks, their customers, and the public to hacking attacks resulting in fraudulent funds transfers using online banking interfaces. These attacks particularly affected commercial bank accounts. For example, the Federal Deposit Insurance Corporation (FDIC) issued an alert regarding this form of attack earlier this year. Both the FDIC and the FBI have recently issued alerts referring to how this hacker attack is being used in conjunction with "money mule" schemes to attempt to hide the fraudulent funds transfers.

In one variety of these attacks, hackers using phishing techniques direct people to spoofed Web sites where malware Trojans are then downloaded to the affected computer. This malware then allows the hacker to infiltrate online banking connections in a manner that can circumvent the customer authentication mechanisms put in place by banks. In simple terms, hackers have figured out how to "hitchhike" on a computer's secure online connection to a bank account and thereby initiate fraudulent funds transfers out of the account. We found a recorded webinar describing how this technique can work using the "Zeus" malware.

Multifactor authentication of the customer has been referenced but not required by bank regulatory guidance as a means banks should consider in protecting online banking systems generally. The guidance does not make technology-specific recommendations but leaves room for banks to make their own risk assessments regarding appropriate security means.

The recent events described above have now raised significant questions about the effectiveness and sufficiency of reliance on multifactor customer authentication as a means to keep fraudulent transactions out of payment networks accessible through online banking systems.

Some view this as another variant of the "whack-a-mole" problem, in which you might smack down one threat but another one just pops up quickly. In other words, we should not throw the baby out with the bath water by disregarding multifactor customer authentication as an effective method to mitigate fraud. Others have suggested the industry should rethink online banking security entirely by investing in systems that authenticate transactions instead of customers, as is common in card transaction security systems. Others suggest systems that provide out-of-band confirmations of transactions (by phone or by text) to avoid overreliance on the online banking channel alone for security.

While banks consider online banking security investments, their customers are increasingly faced with choices about their own use of these systems as they exist today. Some suggest standalone computers running open source operating systems as a security measure. Bank customers can make further use of "positive pay" arrangements with their banks and can better monitor their account activity daily.
Each of these and other available security techniques brings new costs and "frictions" to online banking users. We considered the economic tradeoffs between privacy, data security, and fraud prevention in a prior Portals and Rails post.

At one extreme, some smaller commercial customers of banks may decide not to accept these added costs and instead opt out of online banking access to electronic funds transfer systems altogether if they feel unprotected in this environment. They might even choose to fall back to manual check payments. Is this choice an overreaction or a rational one?

By Clifford S. Stanford, assistant vice president and director of the Retail Payments Risk Forum at the Atlanta Fed

- November 16, 2009 in
  - payments risk
  - supervision and regulation
- Permalink
- Comments