Phishing for the solution to online fraud

In the battle to regain consumer trust in the Internet, victory hinges upon the launch of a multi-pronged attack against phishing and online fraud. By **Alan Pedersen**.

The 'Nigerian' e-mail scam that shot to fame two years ago is unlikely to go down as the greatest con of our times. Like most identity frauds, the goal was to persuade victims into handing over bank account details and copies of their ID, then empty their accounts at the earliest opportunity. The bait used in this particular scam involved the offer of a share in a deal in which the assets of deceased millionaires would be 'liberated' from Nigerian banks and then laundered through the victims' own bank accounts.

Although plenty were hooked in, it was a crude piece of fraud, too amateurish to be a threat to anyone but the gullible and the greedy. But while its success was limited, the scam contained the seeds of what would be developed into something far more sophisticated and intelligent - a form of fraud that is costing consumers hundreds of millions and ruining their faith in the e-commerce machine.

Phishing – a term penned by the hacker community – is essentially a confidence trick enabling criminals to learn enough about their victims so that they can access their accounts or set up new ones by stealing their identities. The most successful attacks trick consumers by hijacking the brands of high profile companies. Fake e-mails claiming to come from reputable banks or online traders ask recipients to confirm their account details via 'spoof' websites designed to replicate the original site. The main corporate targets to date have been financial institutions such as CitiBank and HSBC, although the likes of AOL and eBay have also fallen prey to brand hijacking.

The criminals behind phishing attacks are becoming ever more adept at creating convincing websites that mirror the look, feel and language of the original versions. Maxine Holt, Senior Research Analyst at Butler Group, says that unless they are seasoned Internet users, consumers are unlikely to be able to tell the difference. "They are certainly increasing in sophistication," she says. "It used to be quite easy to spot phishing e-mails and spoof websites. But not any longer."

> The criminals behind phishing attacks are becoming ever more adept at creating convincing websites that mirror the look, feel and language of the original versions.

In a recent Ponemon Institute survey, sponsored by privacy seal provider TRUSTe, around 70 per cent of US consumers said they had inadvertently clicked through to a spoof website. 16 per cent admitted that they had been duped into handing over information such as credit card and social security numbers, or bank account details.

16 per cent represents a good return on investment for these criminals and the reason why experts predict the attacks will continue to rise. The Ponemon survey notes that 76 per cent of respondents had noticed an increase in phishing attacks, with 35 per cent receiving fake e-mails at least once a week.

A matter of trust

Fran Maier, Executive Director and President of TRUSTe, makes the conservative estimate that around 500 million dollars have been lost through phishing-related incidents. But it is the damage to consumer confidence in e-business which she identifies as the key threat. "Between spam, spyware and phishing, consumers are getting fed up," she says. "It is destroying trust."

It is a huge problem for financial institutions trying to move their customers over to low cost, low maintenance Internet banking. Banks may not be responsible for phishing attacks, says Maier, but once an incident occurs consumers' start to question their ability to safeguard online accounts.

In fact, the Ponemon survey reveals that the vast majority of consumers believe online business should be more proactive in protecting their customers. They want to see organisations deploying a range of solutions, from better consumer education, cooperation with law enforcement agencies, to use of technology that can identify fake e-mails and websites.

But is this perception fair – does business need to be more proactive? Dr Larry Ponemon, author of the survey, says that in reality companies have little control over phishing scams. "The general public, however, think that large companies already have certain tools to prevent cyber criminals from using the company's good name, logos and other organisational trademarks."

Because it has borne the brunt of phishing attacks, the financial services sector has been very responsive to working on remedies, says Dr Ponemon. But other sectors that are relatively new to the experience may get caught out. "I think companies in other industries might become better targets because

Five Phishing/Spoofing facts

1. July 2004 figures show that most phishing attacks originate from the United States (35 per cent), followed by South Korea (16 per cent) and China (15 per cent) - *Anti-Phishing Working Group*

2. CitiBank is the most targeted company. 46 per cent of phishing attacks use the Citibank brand to entice consumers into handing over personal information - *CipherTrust*

3. The average lifespan of a spoof website is 6.4 days - *Anti-Phishing Working Group*

4. 76 per cent of consumers have inadvertently visited a spoof website - *Ponemon Institute*

5. 94 per cent of US consumers feel that their bank/credit card company have a responsibility to protect them from online identity theft, but only 52 per cent believe they are doing enough - *MailFrontier*

many Internet users in the United States are becoming savvy to fake e-mails from 'so-called' banking organisations."

Education and awareness

Once incidents occur, organisations are "being pretty quick to contact customers they think have been affected," says Fran Maier. "But I think there are companies who might be in denial, who don't want to say anything about it because they're afraid of the brand value loss." But they needn't necessarily be worried. Being upfront with customers and proactively tackling the issue can enhance a company's reputation, argues Maier, who points to the example of CitiBank which, following numerous attacks, now runs a consumer education programme on its website.

Most affected companies adopt similar strategies for alerting customers, often posting home page notices informing them not to respond to e-mails that ask for personally identifiable information. But Butler Group's Maxine Holt suggests their actions have tended to be reactive rather than proactive. Instead of responding to incidents after the event, she argues that high-risk companies such as banks should be preempting attacks. "It's all very well telling customers that you may have been subjected to a phishing attack…[but] it's far better to give them some warning first."

Consumer and industry groups are starting to get more active on consumer education, says Maier, and there are plans by a group of US non-profit organisations to launch a major consumer education programme. But overall, she says that more effort and collaboration is needed to raise awareness and arm consumers with the knowledge they need. "We have to send a positive message," she says. "Get it out loudly, and get it out consistently."

Expanding the technology front

96 per cent of the consumers in the Ponemon Institute survey want to see technology that will enable them to identify fake e-mails and websites. E-mail authentication solutions such as the Sender ID Framework are being touted as one possible answer. By matching incoming e-mail addresses against the domains from which they were sent, users are able to verify senders' identities. So when an Internet user is contacted by eBay or PayPal they are able to tell that the message is legitimate and hasn't been spoofed.

Despite a number of competing technologies, rows over licensing rights and the absence of an approved standard from the Internet Engineering Task Force, e-mail authentication is starting to draw support from the business community. During October, messaging security firm CipherTrust reported a 75 per cent increase in the take-up of authentication technologies by Fortune 1,000 companies. And in an open letter to FTC chairman Deborah Majoras in November, a 35-strong industry coalition that included the likes of Microsoft, Cisco and Amazon, announced its support for the rollout of a global e-mail authentication strategy.

But the technology is not foolproof, stresses Andy Klein, Anti-Fraud Product Manager for MailFrontier, an e-mail security solutions provider. Authentication can filter or block e-mails whose addresses don't match the domain from which they claim to have come, but persistent criminals have found ways to bypass these systems, he says. Phishing attacks can be launched from legitimate domains that haven't been falsified, or sent out via zombie computers (PCs which have been hijacked by hackers).

"This does not mean that e-mail authentication is useless," adds Klein. "To the contrary, it forces phishers to take additional steps to be able to send phishing e-mails, which may dissuade many phishers." Instead, he suggests that authentication should be considered as one element of a "complete solution", to be combined with other systems such as accreditation (trusted third parties which vouch for the legitimacy of the e-mail sender) and reputation (blocking or filtering of e-mails based on the reputation of the sender's domain).

Ant Allan, Research Director at IT analyst group Gartner, says reputation systems will play an important role in identifying phishing attacks. "Knowing for sure which domain an e-mail has come from is not enough," he says. "You also have to know whether that domain is legitimate, whether it has got a reputation as being a source of spam and phishing attacks."

> "Spam was the beginning, and the increasing sophistication of spam was the next step. And we're seeing that now with phishing." - **Ian Black, Aungate**

Reputation systems, however, are still in the early stages of development and also have their downside, continues Allan. As well as bypassing authentication filters, phishing attacks launched from zombie networks could also slip through reputation systems' controls.

Aside from e-mail solutions, Allan suggests businesses can cut the success of phishing attacks by improving the way in which they authenticate customers who logon to their websites.

Continued on p.17