

(Originally published 19 February 2007 in the Isle of Man Examiner)

TECH TALK with Sherrilynne Starkie

Stop phishing around

Each morning I boot up my computer, open up Outlook, and find at least 35 offers of cheap loans, pleas to clarify my PayPal account details and notices of countless lottery wins. I'll bet it's the same for most people.

But it's more than just an annoyance. It's fraud. And it's very big business with some estimates putting revenues at US \$105 billion a year. The continuing growth in this phishing, a criminal activity using social engineering techniques to fraudulently acquire sensitive information, demonstrates how effective the Internet is for crooks in targeting financial companies.

There are hundreds of phishing attacks each month targeting banks, financial institutions and retailers around the world. Microsoft recently claimed there were 7,000 separate phishing sites in operation at any one time. Each sends out millions of emails purporting to be from real banks. In fact, every High Street bank in the UK has been attacked, as have banks in the US, Australia, Germany, France and Spain, Singapore, China and Japan.

The practice is becoming more sophisticated too. There is a big difference between spearphishing, where a few individuals are selectively targeted, "puddle phishing", which is aimed at very restricted target groups, such as the customers of a retailer and the familiar catch-all phishing attacks, which snare anyone they can from the millions of customers of a major national or international bank.

The recent emergence of Spearphishing is particularly sinister. It targets large organisations, though the ultimate victims are often the individual customers who find their personal data has been stolen. In these cases, well-researched, carefully customised emails are sent to the employees in a large company or public sector organisation who may be dealing with customer details or financial data and who could be persuaded to click on an apparently innocent link. That click allows aggressive malware to attack crucial parts of the corporate system so that data can be harvested by the fraudsters.

Organising these attacks takes a lot of technical expertise and knowledge of the workings of the finance industry and large organisations. So who's behind it? Some say it's organised crime gangs, generally from Eastern Europe and Russia.

"A complex lifecycle structure has grown up around the areas of phishing, spam, malware and DDoS attacks, and it takes quasi-military discipline to ensure everything goes to plan," explains Ben Coppin, founder of Envisional, an Internet intelligence company that is expert in artificial intelligence technologies. "There are some freelancers, and plenty of incompetent amateurs keen to chance their luck. But they are almost irrelevant to the big picture. It is the major criminal organisations that set the pace and cause the real problems."

The people in these gangs who are busy sending out spam emails, operating botnets (networks of PCs that are hijacked and used for spamming and DDoS attacks) and selling information on IRC (Internet Relay Chat) channels are very junior players. These minions are paid per item or per attack and are part of a complex criminal pyramid. It's only a few crooks at the very top that make the real money in phishing.

People are getting smarter and the computer security in banks more sophisticated. So will phishing soon be relegated to the annals of criminal history? I don't think so. As technology

improves and security standards are raised, these gangs will redouble their efforts to find more sophisticated ways to challenge defences. That they have the technical resources there is no doubt. And because humans, by their very nature, are the weakest link in any security system, there will always be workarounds for criminals to exploit.

Still there is hope. Clearly better security and identity management technologies are being implemented. More international cooperation and better education to increase business and consumer awareness have been crucial in countering attacks. So, the key is to keep raising the bar for the fraudsters, to make their jobs harder.

-ends-

Sherrilynne Starkie is the managing partner at Douglas-based Strive Public Relations, a virtual communications consultancy serving the Island's tech sector. She provides her views on business and technology, and the business of technology, each week in Tech Talk. Visit her business blog, Strive Notes for frequent updates. www.strivepr.com

(707 words)