Who'd Phish from the Summit of Kilimanjaro?

Richard Clayton

University of Cambridge, Computer Laboratory
richard.clayton@cl.cam.ac.uk

Phishing emails are now so convincing that even experts cannot tell what is or is not genuine[1]; though one of my own quiz answering errors resulted from failing to believe that genuine marketeers could possibly be so clueless! Thus I believe that education of end users will be almost entirely ineffective and education of marketing departments – to remove "click on this" (and HTML generally) from the genuine material – is going to take some time.

Providing end users with one-time passwords (pads of single-use numbers, SecurID tokens, PINs sent by mobile phone) can ensure that phishing only works when there is a real-time, Man-in-the-Middle (MITM), attack. This will immediately deter the bad guys if their technical expertise runs solely to copying websites. However, formal analysis of online banking protocols shows that only a handful of the "bag of bits" being passed around can be considered to be authenticated – and so a MITM can, unhindered, steal whatever they wish.

Insisting on SSL (`https`) connections will prevent the use of random URLs for phishing websites and bring the focus back to control of the DNS. However, once the second level (`fakebankname.com`) is secured then the attackers will just move down a level (to `bankname.plausible-second-word.com`). I predict a lot of wasteful activity before the nature of DNS delegation is fully understood.

Insisting on client certificates prevents MITM attacks, but also stops me paying my gas bill from a holiday cybercafé – which is bad for business. But why do I need the same authority to pay the bill as to change the name of the gas company? A range of authentication systems is needed, chosen as the risk varies. The banks could learn from the activity monitoring systems of the credit card companies, and ensure that extra authentication is seldom necessary or onerous. For example, a check can be made on the IP address of incoming connections. If the session arrives from a cybercafé in Latvia or a web hosting rack in suburban Moscow then Mr. Jones in Acacia Avenue is not connecting directly... if he really does want to set up a new payee then perhaps he could ring his branch and confirm that he's taking an East European holiday?

To conclude; I can see no silver bullet (I can imagine success for phishing emails that ask for client certificates), and most of the proposed argento-ammunition is useless once the end-user machine is compromised. Nevertheless,

[1] MailFrontier Phishing IQ Test II `http://survey.mailfrontier.com/survey`

A.S. Patrick and M. Yung (Eds.): FC 2005, LNCS 3570, pp. 91–92, 2005.

a blend of security improvements will freeze out all but the most competent criminals. Society may need a general solution to online security, but the banks only have to persuade the bad guys to move on to more attractive targets. However, the fixes must *not* be introduced one by one, allowing each to be overcome individually. What's needed is a 'Kilimanjaro effect', where the security suddenly dominates the landscape and it will always seem to be a long way to the summit.