Phishing - What it is and How it Will Eventually be Dealt With

By Ian Grigg, Financial Cryptographer

Web: Financial Cryptography
Email: *iang at systemics dot com*

Ian Grigg has been a Financial Cryptographer since 1995, building strong payment and real time trading systems for exotic instruments, in Europe, the Caribbean and North America. He is the author of the influential 7 layer model that integrates technology to business in digital commerce. He is currently working on new definitions in security and governance, as well as systems to integrate payments with instant messaging. He has a BSc(Hons) Computer Science from the University of New South Wales and an MBA from London Business School.

Abstract

Phishing is an attack on the user and her browser. Addressing phishing necessarily means changing the browser, and this creates tensions between those who lose money - users and ecommerce sites - and those who need to do the work - browser manufacturers.

Intro

The Internet has suffered various attacks for some time such as spam, cracking (or hacking), denial of service and the like. Yet, for the most part, these have been nuisance attacks, and have resulted in disruptions of service, and only loose or minimal economic benefit to the attackers.

Phishing changed all that. Although its antecedents go back to 1997 or thereabouts, modern day phishing on a large scale started around 2002. By the beginnings of 2004, it was an unstoppable machine, and by the start of 2005, phishing was industrialised in the sense of organised crime.

Phishing was also different because it stole money. It was clearly fraud, rather than damages by indirect effects. But, more than that, stolen money meant that the rewards from one successful event could be invested into the next one, and hence phishing is a self-sustaining and profitable industry (Ref: Grigg, The Year of the Snail).

As users as well as the executives and technical staff in ecommerce companies, banks, police forces and regulators struggle to cope with the epidemic, it behoves to have a very clear view of just what phishing is. Only then can the victims move to defend against it. This note will describe that, and then propose how phishing will be addressed in the longer term.

The Browser's Security is being Attacked

Phishing is an attack on the security of the web browser. The original security design, crafted a decade ago by

Netscape, RSADSI and VeriSign, promised to protect the user from spoofed websites. This was perceived as an essential element of protecting the data in delivery from the user to her trusted online commerce site, because if the identity of the website was not confirmed, an attacker could simply sit in the middle and steal the data by pretending to be the other side to each other.

This Man-in-the-Middle attack has entered the lore of Internet security as the attack we needed to guard against, and it is this attack that the browser falls to. In the case of phishing, MITM (as it is known) is accomplished by the phisher completely avoiding the security of SSL and signed certificates altogether and simply pretending to be a secure website.

Why is it so easy to do this? The original security design protected against this easy spoof by requiring the branded logo of the Certificate Authority (CA) to be presented to the user when the secure connection was set up (Ref: Bob Relyea, post 10 Feb 2005 npm.crypto). But this model was crafted during a time of peace. As time went on, important user elements were dropped from the browser, and now, the only part left is a small padlock that is misunderstood by users or simply ignored (Ref: Friedman, Hurley, Howe, Felten, Nissenbaum, Users Conceptions of Web Security: A Comparative Study).

So it has become an easy task for the phisher to craft a spoof website that confuses the user, and thus acquire her identity information, her account numbers and passwords, or whatever is considered relevant.

Back to the Future of Browsing

Thus, to address phishing, all we need to do is go back to the original security design. In strictly technical terms, that means:

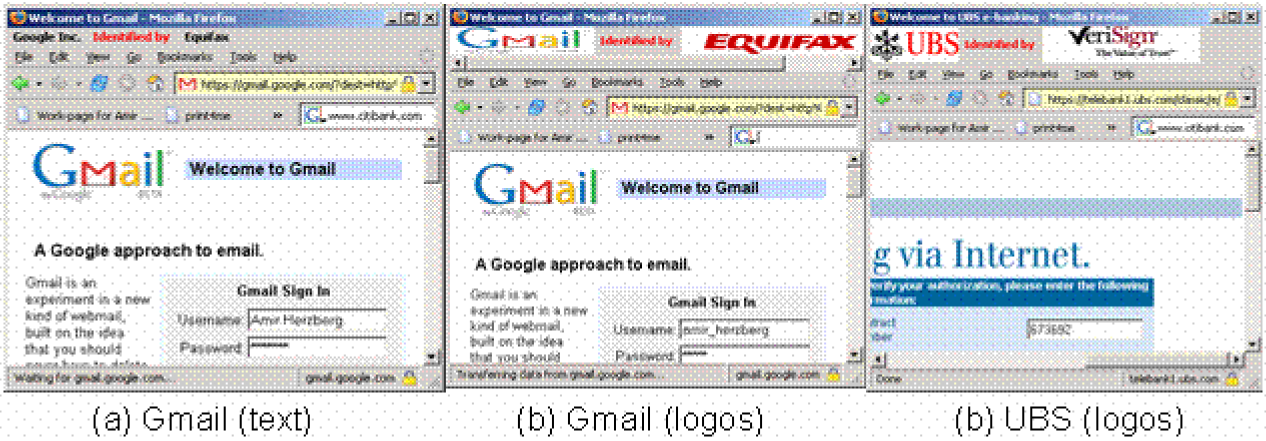
Firstly, employ a range of techniques to make a secured connection obvious to the user: additional status bar information and bold colouring such as is used in Firefox is one way. Our first step is to force the phisher onto a battleground of our choice: SSL and certificates.

Secondly, just exactly who signed the certificate is critical to defending against phishing. This must be presented to the user in a branded logo fashion, so that she can see the information quickly and efficiently.

The importance of this becomes immediately apparent when the phisher is forced to use SSL and certificates. He will then attack with a certificate from a distinct Certificate Authority, using a domain name that is confusing to the user. Now, by engaging the user, she can be expected to remember the branded CA of her banking sites, and any reputable Certificate Authority can be expected to be on the alert for phishing attacks within its own customer base. This second step works because the branded logo is the most efficient way to deliver information to the user about a small number of choices (Ref: Figure 1 shows Equifax and VeriSign, from Herzberg & Gbara, TrustBar: Protecting (even Na?e) Web Users from Spoofing and Phishing Attacks).

Thirdly, we need to further bind the user's relationship to her secure banking site in a more pro-active way. This means that the browser should offer her the ability to make judgements based on her known good sites. One simple way is for her to set a petname (Ref: Marc Stiegler, Introduction to Petname Systems). This means typing in "my favourite bank" for, say, Bank of America, and expecting to see that personal phrase every time she is secured by that certificate.

Better than a petname is a graphical image selected by her, as graphics provide a much more efficient delivery of security information to the user (Ref: Herzberg & Gbara). If her chosen image is not present, alongside the logo of the CA, this can be seen by the user as a sign of danger.


Welcome to Gmail - Mozilla Firefox
Google Inc. Identified by Equifax
File Edit View Go Bookmarks Tools Help
https://gmail.google.com/?dest=http
Work-page for Amir ... print4me
www.citibank.com
Gmail
Welcome to Gmail
Waiting for gmail.google.com...
gmail.google.com
Welcome to Gmail - Mozilla Firefox
Gmail identified by EQUIFAX
File Edit View Go Bookmarks Tools Help
https://gmail.google.com/?dest=http%
Work-page for Amir ... print4me
Gmail
Welcome to Gmail
Transferring data from gmail.google.com...
gmail.google.com
Welcome to UBS e-banking - Mozilla Firefox
UBS identified by VeriSign The Value of Trust
File Edit View Go Bookmarks Tools Help
https://telebank1.ubs.com/classic/
Work-page for Amir ... print4me
www.citibank.com
Done
telebank1.ubs.com

A Google approach to email.

Gmail is an experiment in a new kind of webmail, built on the idea that you should

Gmail Sign In

Username: Amir Herzberg

Password: •••••••

A Google approach to email.

Gmail is an experiment in a new kind of webmail, built on the idea that you should

Gmail Sign In

Username: amir_herzberg

Password: •••••

g via Internet.

erify your authorization, please enter the following rmation.

673692

(a) Gmail (text) (b) Gmail (logos) (b) UBS (logos)

Figure 1. Engaging the User

This final step works with sites that are known to be trusted and good by the user. That's because any phishing attack generally seeks to attack a valuable relationship that is already in existence, so leveraging that relationship is key to protecting it.

In conclusion, it is important to stress that these steps are both within the original thinking of the security design, and have also been tested in experiments as shown in Figure 1 (Refs: Herzberg & Gbara; Friedman et al). They simply lack widespread deployment in today's browsers.

How then to Deploy?

If it has not become abundantly clear by now, it should be stated in the clearest terms: Users and Executives of ecommerce companies and banks are almost completely powerless to effect these changes. Yet they carry all of the cost for shortfall in security in the browser. There are two paths by which these changes are then to eventuate.

Microsoft recently announced a mid-year security update, with an emphasis on phishing protection (Refs: Smith, IT Manager's journal; Grigg, A Blackbird Moment). I have no doubt that they will incorporate these ideas into their product. Opera recently released a browser that brands the CA onto the browser for secure connections. Mozilla are experimenting with making the SSL connection more obvious.

It will probably take another year before widespread deployment is achieved. And that won't take off until Microsoft release their anti-phishing browser release, slated for mid 2005. We may have to wait until mid 2006 before phishing comes under control via the natural forces of evolutionary rollout; and so we can expect a year's worth of additional phishing losses at $1.2 billion per year (Ref: Gartner/Litan Seattle Times).

The second path is by litigation. Recently, a user sued his Florida bank for a transaction initiated from his machine, under malware influence (Ref: IHT; BG; IS). Similarly, the Choicepoint scandal out of California is another one to watch. Both of these developments are being closely watched by class-action specialists, and within the next year, we can expect the banks to have to deal with phishing in the courts.

And, we also can expect banks and ecommerce companies to consider this unjust, as they have no great control over the software tools in question. In order to defend themselves from growing damages in phishing, these companies are going to have to go to the source of the difficulties, the manufacturers of the browsers. This will be costly and distracting, and may not in the long run help the real goal of securing the user and the banks against phishing.

Far better for ecommerce companies and banks to get pro-active now, and pressure the browser manufacturers. How this is done is up to the executives of these companies. But consider this: if a letter from your lawyer to Microsoft's lawyer questioning the latter's progress in anti-phishing were to bring forward the deployment of these techniques by a mere month, this would save $100 million.

That's probably worth the lawyer's fee.