# Phish and Chips: We're with Bill Gates -- We'll Never Fix this Problem without Smart Cards

**By Dave Birch and Steve Pannifer, Consult Hyperion**

Web: http://www.chyp.com
Email: dave.birch@chyp.com or steve.pannifer@chyp.com

You can't have failed to notice reports of a major Internet crime wave underway on both sides of the Atlantic at the moment: phishing. This means duping consumers into divulging financial information using spoof web sites [1]. In non-cool, un-hacker terms, the fishing involves sending out spam e-mails to try and tempt unwary consumers into visiting the fraudsters web sites.

Every single Internet user must have received hundreds by now. You know the form: hello, this is Citibank (or whoever) and we're just checking (or whatever) our security system, so please click on this link and enter your username and password (or card number and PIN, or whatever).

The link is, of course, not to the bank but to the fraudsters' web site. Once the customer enters their details, the fraudsters whisk them away for their own use: this use generally being to loot the bank account as quickly as possible. If the fraudsters send out 10 million e-mails, and 1 in a 100 of the hapless recipients is a (for example) Citibank customer, and 1 in a 100 of them is fooled by the e-mail, that means that the fraudster could gain access to a hundred Citibank accounts. And they do. In the UK, Lloyds TSB, NatWest and Barclays have all admitted that customer accounts have been accessed and that money has been stolen but none of them would give a figure. APACS say that they think the figure is over a million and still growing [2]. And this stolen money isn't the only cost to the banks, who also have to pay to repair the damage: changing names and passwords, re-issuing cards, reassuring customers and so on. This has already cost some �60m in the UK [3] and, according to research company Gartner, more than a billion dollars in the US last year [4]. According to The Nilson Report, a respected industry newsletter, a list of 200 million e-mail addresses can be purchased for �20 or so and (of that fraction of the 200 million who are actually customers of the "target" institution, in fact around 7% give up data of sufficient value to be used or sold on). No wonder it's on the rise.

It sounds incredible that people would fall for phishing scams in such numbers, but the sophistication of the attacks is high and growing. In some cases, victims are directed to the real bank web site while a pop-up window is overlaid to capture details. In other cases, the surfer's toolbar is taken over. One of the latest attacks against Barclays goes even further [5]. It involves tricking people into going to a web site that sneakily downloads a "trojan horse" programme to their PC. The trojan horse (which has been written specifically to attack Barclays' customers) watches keystrokes and thus snaffles the customer's identifier and passcode. Because Barclays' log-in then asks customers to enter two letters from a secret word, by choosing them from pop-up menu to defeat key loggers, the fraudster's software takes a picture of the screen and mails it back to them!

What is to be done? Phishing is possible because authentication to online services is so univerally weak, consisting of various PINs and secret phrases all of which amount to nothing more than basic password authentication [6]. As well as this customer authentication being weak, service provider authentication is similarly weak. The very fact that phishing sites work at all proves that the authentication of banking and other e-commerce web sites is effectively non-existent: the fact is that customers need to have as much assurance that they know who they're dealing with as the service provider does about who is logging onto its service.

Against this, it is not enough to assume that customers can be educated and then relied on to recognise fraud when it happens. Warnings are all well and good, but it's just impossible to stop this sort of attack (as in the case of so many other Internet attacks) without better authentication. As Bill Gates said back in 2000 [7], and we've been saying for over a decade (eg, [8]), passwords are the weak link in Internet security and the industry needs to move to smart cards.

But who will provide authentication based on smart cards? In the UK, banks are currently spending hundreds of millions of pounds on just such a better authentication scheme: chip and PIN. As the advertisements ("Security in Numbers") have made clear, chip and PIN is targeted at shops in the real world. But suppose it could be used with your PC, TV or phone as well? And what's more, suppose it could be used without having to have a smart card reader in your PC, TV or phone? That would be a really useful solution.

As is happens, APACS have been developing the specifications for such a solution: it goes by the name of "token authentication". The idea is that your bank would give you a small device, a bit like a pocket calculator, When you want to log in to your bank on the Internet, the bank asks you for a code number: let's call it the response. You put your bank card into the calculator and punch in your PIN: the device displays a code number (the response) which you then enter in to the web site or tell the person on the phone. From this number, the bank knows that you had a real card and entered the right PIN. Since you have to have both the card and the PIN in order to log in, this is known as a "two factor" authentication (as opposed to the "one factor" password).

The token authentication device can also work in another mode of operation. In this mode, the bank sends the customer a number: let's call it the challenge. The customer punches this challenge into their device and then enters their PIN. Another code number (the challenge-response) displayed then depends on both the PIN and the number sent from the bank, not the PIN alone. If the challenge from the bank is dependent on the transaction details specific to a transaction2 then by sending back the displayed challenge-response the customer is in effect providing a digital signature for the transaction.

Interestingly, this usage mode also provides a means for the customer to be certain that they are talking to the bank. Just as the bank can send a challenge to the customer and check the response, so a customer can send a challenge to the bank and check their response. Here's a practical example:

- Fred gets a phone call: "Hello, this is JumboBank calling about your Super Premium Saver Plus account. Can you give me your mother's maiden name".
- Fred, being a suspicious person who has read lots phishing stories in the newspaper says "Who the hell are you? Why should I tell you my mother's maiden name? I challenge you".
- Fred, who already has his debit card inserted in his token authentication device presses a button and it displays a number which Fred punches into the phone.
- JumboBank customer representative says "Our response is 976324".
- Fred punches in 976324. The device says "OK", or whatever, and now Fred knows that it really is JumboBank and can relax and listen to the customer representative who tells him about the new Super Gold Platinum Extra savings account which pays 0.15% gross per annum.

Note that the same process could be used to authenticate between any customer and service provider: someone logging on to the Inland Revenue, as an obvious example. The bank always has to be in the loop (because only the bank has the relevant security keys) and therefore can always charge for the service. Not only a way of defeating phishers and doing away with secret words, but a way of generating additional revenue.

In summary, then, using the EMV cards already issued to customers plus a simple, dumb, calculator-like device (which contains no clever cryptography, remember, as that's all on the card), customers can be sure they're dealing with their bank and banks can be sure that they're dealing with their customer.

## References

1. Anderiesz, M. A big catch in the phishing season in The Guardian (Online section) (29th Jan. 2004).

2. Greenwood, L. E-mail scams costs banks �1m in BBC News (24th Apr. 2004).

3. Warren, P. �60m bill for banks as online phishing hooks the unwary in The Evening Standard (29th Apr. 2004).

4. Gartner Study Finds Significant Increase in E-Mail Phishing Attacks Against U.S. Online Consumers in Business Wire (6th May 2004).

5. New "Purchase Confirmation" Trojan Variant at (on 10th Apr. 2004).

6. Birch, D. Is the end in sight for passwords? in Card Technology. 8(14): p. 18-19 (Dec. 2003).

7. Wagner, A. Gates pushes smart card technology in Nando Times (10th May 2000).

8. Birch, D. Downloading Software, Uploading Money-Business on the Infobahn in proc. of Internet and the Enterprise, Technology Appraisals (London: 1994)

9. Litan, A. Fighting Identity Theft and Consumer Fraud in proc. of ASROC (London: Oct. 2003)