

Software & Systems Identity Theft (Phishing)

Overview

With the increase in the use of internet banking, comes an increase in attacks from fraudsters.

No one would hand over their cash card PIN number to a stranger who came up to them in the street, but we do exactly this when we receive emails that are apparently from our bank.

In general, never divulge any personal details in response to an email, either by replying directly or by following an embedded link to a web site. This may appear obvious, but the fraudsters are becoming very clever. One of the latest scams is called *Phishing*.

Phishing

The *phisherman* creates a false web site that looks identical to the web site that it is impersonating. They will use the same logos and layout as the real site. Even the web site address displayed in the browser address bar, may only be slightly different.

The phisherman then buys (legally) email address lists, and starts sending thousands of emails. The emails will have a fake *from* address that makes it look like it is a legitimate email. The email will ask a user to log into their account, and helpfully provides a link to click on. Never click on this link. It takes longer to manually start up the browser, and type in the address that is known to be true, but it is time well spent. Here is an example shown below.

Click on the link below to visit the BBC web site!

www.bbc.co.uk

The link looks like it will send the user to the BBC web site, but if clicked on it, it will go to the ITV web site instead!

This was not a very clever deception and it would have been quickly noticed that it was not the BBC web site, but imagine how easily a user could be fooled if the fraudster had used the same logos and layout as the real BBC web site.

The first thing that a user will be asked to do when entering the false site is to log in. This gives the phisherman private and confidential username and password details. The phisherman takes these details and logs onto the real web site ... well you can imagine the rest.

A dangerous new type of phishing attack replaces the "Address" bar at the top of a Web browser with a working fake, using JavaScript. This technique allows the phisher to display a completely fraudulent Web address URL, while taking the user's browser to the phisher's own, spoofed site. The fraudulent site can be strikingly convincing, as the "Address" field in the browser displays a URL that appears to be a secure link to the trusted brand's web site, e.g. "https://".

Since the fake "Address" bar of the browser remains installed after leaving the phisher's site, there is a possibility that a phisher could use this technique to secretly track every web site the user visits next. Some of the well-known brands that may have been abused to lure unsuspecting Internet surfers in recent months are eBay, Citibank, Paypal, AOL, Visa, Microsoft, HSBC, Lloyds, Yahoo, and AT&T. The first **virus** applying the phishing technique has surfaced just recently.

What to do next?

The safest way to access a web site is to always manually enter it on the browser address bar. Clicking on links embedded in emails is dangerous.

Bookmark bank web sites etc in browsers. This makes it less likely that a user will take shortcuts and click on links. It also prevents the user from going to the wrong site by mistyping the address.

Help Accountants will never send an email asking the user to log into their web site, and they will never ask a user to reply to the email with usernames or passwords. Similarly neither will any of the banks, eBay or PayPal services.

Upgrade to the latest version of an Internet browser. The latest versions of Internet Explorer and Firefox have hoax address detection mechanisms.

More Reading

To read more, visit the following sites. Note that these are real addresses. Trust us!

Anti-Phishing Working Group (APWG) <http://www.antiphishing.org>

The National Hi-Tech Crime Unit <http://www.nhtcu.org>

Bank Safe Online <http://www.banksafeonline.org.uk>