# Anatomy of a phish - how crooks hack legitimate websites to steal your details

Naked Security post from Sophos Asia Pacific Head of Technology Paul Ducklin

Old-school phishing is where cybercrooks lure you into logging in to your bank account on one of their websites.When you enter your personally identifiable information (PII), as you would on the bank's real site, it gets uploaded to the crooks instead of to your bank.

The idea, of course, is that they then use the credentials they just stole to start draining your account.

So phishing is still worthwhile to the crooks, even though it doesn't seem to be quite as successful as it used to be. Many of us have learned to take great care when we're banking online, and to check for the "vital signs" of a scam before we trust a website with our usernames and passwords.

Nevertheless, the phishers are still giving it all they've got. By combining simplicity with accuracy, they're creating banking scams that are much more believable than the crude and misspelled emails and websites that were common a few years ago.

If you pick your moment, or just get lucky, there's still money to be made.

In Australia, for example, today (at least in Sydney) has been a very wet and gloomy public holiday.

Just the sort of morning to loaf on the couch with your laptop or your iPad and goof off online, where you might have received an email like this one:

Many banks now have a closed cloud-style email service built into their internet banking sites. The idea is that you'll get into the habit of logging in securely to read important messages, rather than believing what arrives in insecure emails.

The bank still sends you emails, but they don't contain any detail - they just give you an overview (e.g. "your statement is ready"), and advise you to read the full message on the secure site. A bit like the message here, in fact.

But what your bank won't do is to invite you to click a link to get to the secure site. They rightly leave you (indeed, they urge you) to find your own way to the banking portal, so you're not at the mercy of the URL embedded in the email.

So the link here is certainly phishy - it shouldn't be present at all - but it doesn't look like the sort of obvious phishing nonsense you often see.

You probably know what I mean: weird and unlikely domains such asreally.your.bank.wefljdrsecxr.example.org that are an instant giveaway of bogosity.

In fact, this phish links to a government website in .cn (that the People's Republic of China, or PRC):

The government site seems to have had a security lapse, allowing the crooks to add a small and simple web page called nabau.html.

This page silently redirects your browser elsewhere by using this HTML:

The redirect takes you off to another hacked site, specified in the URL as an IP number rather than as a domain name.

This presents you with a bogus login page hosted on a web server (it looks like part of the Computer Science department) at a Colombian university:

Ironically, this bogus page helpfully advises you to keep up to date with anti-virus, firewall software and the latest patches, and urges you to report phishing scams to NAB.

When you click Login to submit the form, the POST request (HTTP's name for an upload) goes to yet another hacked web property. This one is a student vacation site in the USA, apparently with some insecure plugins in its blogging subdirectories.

You never get to see the site's main page, which is unexceptional:

Instead, the web upload that is linked to from from the Colombian university page gives the crooks their first page of login data.

Then you're shuffled back to the server in Colombia to face a request for another page of PII:

The POST request on this page uploads your formful of data to the same place as before: the US student vacation site.

This time, the vacation site bounces you back to Australia, rounding off the phishers' journey.

You end up unremarkably on National Australia Bank's own site, albeit that you're on the regular main page, not amongst the internet banking pages:

Let me be quick to say that you ought not to fall for this sort of phish:

NAB wouldn't have put a link in the email, so you ought not to have clicked it.None of the so-called banking sites referenced a nab.com.au URL.None of them used secure HTTP, also known as HTTPS.(HTTPS is the protocol that puts a tiny padlock in the address bar at the top of your browser's screen.)

Nevertheless, this phish didn't take you to any sites that would have stood out, under normal circumstances, as part of the cybercriminal underworld.
It relied on three unremarkable and legitimate servers, owned by legitimate organisations and operated by unsuspecting sysadmins, in three different countries: PRC, Colombia and the USA.
That's why even self-proclaimed "safe surfers" - people who back themselves not to wander off into obviously-shady parts of the web - should consider themselves at risk.
Be careful out there. And that applies whether you're browsing or running an online business.
The crooks want to redirect your browser into harm's way, and they want to use your servers to help them do so.

Full post available
at: http://nakedsecurity.sophos.com/2013/01/28/anatomy-of-a-phish-three-legit-servers-in-three-different-countries-borrowed-by-the-crooks/?utm_source=feedburner&utm_medium=feed&utm_content=Google+Reader&utm_campaign=Feed%3A+nakedsecurity+%28Naked+Security+-+Sophos%29