Online Shopping and a Phishing Pheeding Phrenzy

David Harley, ESET Senior Research Fellow
Urban Schrott, IT Security & Cybercrime Analyst, ESET Ireland

Introduction

One of the earliest projects David Harley worked on at ESET was a paper on phishing with Andrew Lee – A Pretty Kettle of Phish, published in 2007. They worked on a number of related papers subsequently, and the problem hasn't gone away (indeed, it comes up time and time again in our blogs).

In fact, according to the Anti-Phishing Working Group's most recent report, while the number of PCs infected by phishing malware was decreasing in the first quarter of 2012, the number of unique phishing sites flagged by the APWG reached an all-time high of 56,859 in February, with another all time high of 392 targeted brands in February and March.

However, like other threats primarily based on social engineering, phishing doesn't stay in one place for too long: it changes attacks and vectors. When that paper was first written, social media like Facebook and Twitter were much less used, whereas they're now routinely used as a channel for phishing and other attacks. Which means, perhaps, that ESET should consider revisiting the issue in a new or re-engineered paper, but in the meantime, here's a recap along with a discussion of a new twist or two, courtesy of recent research by Urban Schrott, IT Security & Cybercrime Analyst at ESET Ireland.

Phishing and Identity Theft

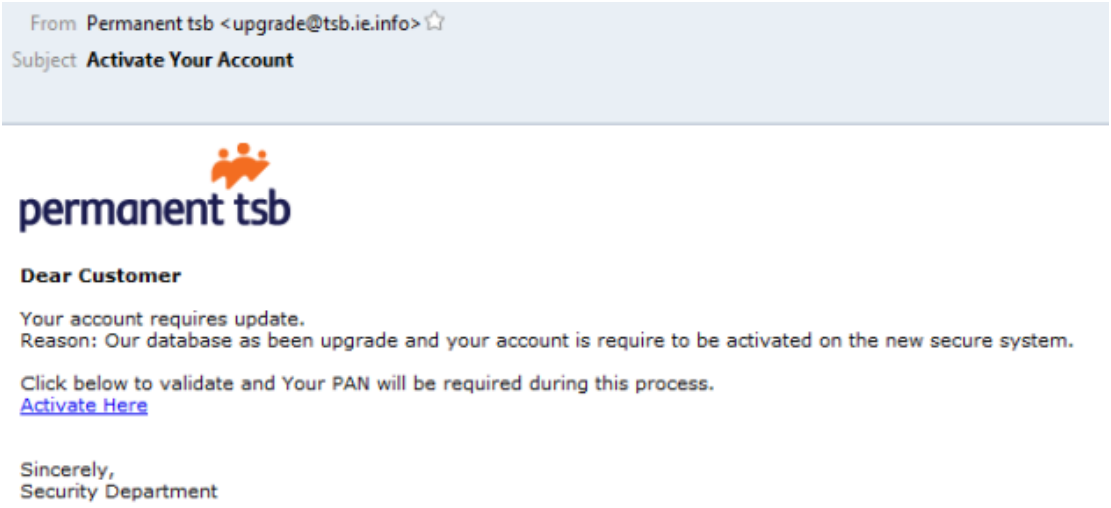
Identity theft in one form or another has been around far longer than the internet, of course, but phishing doesn't require a complete assumption of the victim's identity (the sort of thing pushed to extremes in the plot of The Net). More often, it involves sending some sort of message taking on the identity of an (often real and legitimate) organization or person as part of the process of

obtaining sensitive information from a potential victim in order to perpetrate fraud and/or further identity theft (which might indeed be far more extreme, but phish gangs tend to favour less dramatic attempts at impersonation of a victim, if only to reduce the risk of early discovery).

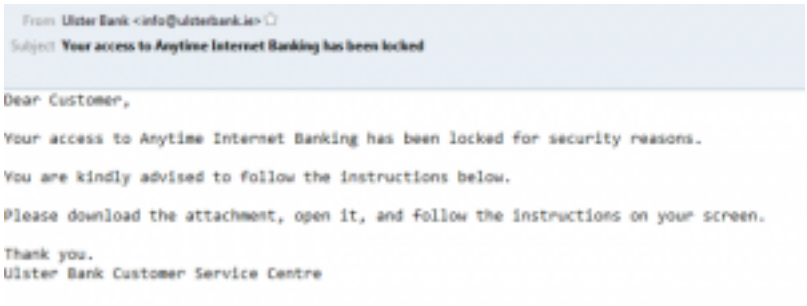
The posting of a deceptive message is only part of the phishing process: equally important is the dishonest acquisition of data from fake web sites or other data capture methods, including fake forms, keyloggers, backdoor Trojans and so on. While phishing is often about finance-related institutions (banks, credit unions, Paypal, auction sites and so on) we should not assume that target data is always related to the victim's personal finances. In principle this kind of attack can be intended to access quite different forms of data – industrial espionage, ISP account info, info relating to access to restricted systems, and so on – and may be highly targeted. (Sometimes we refer to this as spear phishing, but that's a topic for a separate blog.)

Phishing from the Banks of the Liffey

Here are a couple of examples of basic bank phish messages highlighted in a recent blog by Urban Schrott, of ESET Ireland.
The first one contains a link to what appears to be the Permanent TSB web site, but is actually a fake designed to con the victim into giving up his login credentials.



The second example arrives as an attachment to an old-school, visually unconvincing message like the one below, allegedly from the Ulster bank, which is apparently so poor it can't afford a logo…



While the message is pretty crude, the attachment is the more convincing form shown below: at least, it *looks* reasonably official. When we look at the content, however, it turns out that you're expected to enter everything a crook might need to access your bank account, including your PIN and your mother's name (presumably this is for the infamous supplementary question "What was your mother's maiden name?"

This is an important distinction: as a general rule, when a bank (or any other institution) asks you for your password for purposes of authentication, then by definition it wants you to give enough information to prove that you're who you claim to be. It doesn't need a whole load of other information just to be on the safe side. This isn't actually the 'greediest' example we've ever seen: some also demand full contact information, your social security number, date and place of birth, and your favourite shade of green. (Favourite shade of green is an exaggeration, but only slight…)

So far, so unpleasant, but pretty standard as phishing goes. However, here's something a little different.

Selling Online: Avoiding the Scams

ESET Ireland has recently come across examples of phishing attempts in replies to classified ads on Donedeal.ie. (However, you'll come across the same sort of thing as a user of eBay, Craigslist and so on.)

The seller may receive an innocent looking message like *"Is the item still for sale?"* and if he replies, he's likely to receive a generic answer such as this example:

> Hi mate, I have looked at it a few times now, and after looking around, I'm satisfied with the great condition but what's your actual price for it. I love a bargain, so i would like to get it as soon as i can. I would be able to make payment through PayPal, i find it the easiest way to use my credit card safely and is a safe and reliable method of payment... Let me know your price for it . I hope to hear from you soon, and i will make all transportation preparations for the it to be transported to my home. If possible can you send me some recent picture of the item ?

All At Sea

In the case above, the seller was selling a boat, but if you read the reply, the buyer doesn't mention the boat at all, he keeps referring to "it", or "the item" (or even "the it", presumably a typo for "it" or "the item"). This suggests that the message is a generic (i.e. non-specific) reply sent more or less automatically to a large number of sellers of all sorts of items for sale. (A lack of personalization is one of the main giveaways when it comes to most kinds of – non-targeted – phish.)

Part of the purpose of the scam may be to engage the seller to disclose their online payment account details and other personal information, which the scammers can then use for identity theft, attacking their account and other activities from which they can get financial gain. However, there's usually a second phase of the attack, where the scammer follows up from another email address with a phishing email appearing to be from PayPal (or Craigslist, or whatever service is being used.) In some cases, the scammer will have asked for a payment invoice request. However, in this phase, the detail of the message will obviously vary widely.

However, a complete example will probably look something like this, albeit with graphics and pseudo-legal textual frills to make it look more official:

> *Dear* [victim's name]
>
> [Service provider] *confirms that* [scammer's alias] *has sent you* [agreed sum, often in excess of the amount for which the item was originally offered] *for* [the item].

[Victim's name] deserves a little clarification. Initial phishing emails normally use something like 'dear valued customer' or the victim's email address because they don't have access to a real name. (One of the likely indicators of a scam is non-personalization.) In this case, however, the scammer may be able to use the victim's real first and last name correctly, as derived from the victim's response to the original phishing message. This may make it harder to distinguish from an authentic PayPal message.

The details of the item and the transaction will be included, to reassure the victim that all is correct. However, there will also be a note to the effect that payment is pending for some fabricated reason (usually to do with security – it's amazing how often security is eroded for 'security reasons'). The note will state that the provider will not credit the victim's account until the shipment reference number has been received, in order to protect the buyer from fraud on the part of the seller. However, the odds are that the scammer will receive and sell on the goods without paying any money whatsoever.

There may be a pointer to the real PayPal site, on the assumption that the victim will be reassured by the official look of the message and not seek verification. However, it's at least as likely that the pointer will be to a cloned PayPal site giving misleading information. In such a case, the scammer not only gets the goods without paying, but may be able to carry out other fraudulent activities before the victim realizes that he's been conned.

Urban Schrott asked PayPal about such dodgy offers and the abuse of PayPal name for scamming activities and they replied:

> `You're right – it was a phishing attempt, and we're working on stopping the fraud. Identity thieves try to trick you into`

revealing your password or other personal information through phishing emails and fake websites.

Buyers and sellers through online classifieds should therefore always check the identity of the person with whom they're dealing with, how safe their methods of payment are and if they're unsure of anything, they should always check with the service first. They should take advantage of the fact that reputable companies like PayPal offer a means of securing transactions without giving away information that makes it easier for the scammer to pretend to be a service provider. They should take the time and trouble to find out exactly how the service protects *both* parties in the transaction. And in most cases, we recommend that they link their credit cards rather than their cheque or savings accounts, as they're likely to get better protection/recompense in the event of a successful fraud.

Phish Avoidance

Here's a shortened and updated version of the advice that David Harley and Andrew Lee gave to potential phish victims in an earlier paper.

The infographic isn't from the paper, but has been used by ESET before, notably in a blog article by Randy Abrams. You may still find it useful, but bear in mind that phishing is by no means restricted to email messages, and that sometimes the real danger is in the attachment, which may be some form of Trojan or contain malicious links that aren't present in the message.

- Email sent apparently from a provider you don't use is obviously suspicious. However, if you receive email apparently from a services provider that you do use but at an address that you do *not* use when you contact that particular bank or service is *always* suspicious. One precaution is to create a separate email address (most ISP's will allow this, but you could also use a service such as Gmail to create extra accounts), with a unique name, e.g. (mybanking.email@thedomain.com), and use that address exclusively for that activity, never publishing it anywhere or using it to send email for other purposes. This will provide an easy way of checking that it was sent to you at a correct address.
- If you do have an account with the institution apparently sending it to you, but the message isn't personalized – that is, addressed to you using your own name or a specific identifier such as a verifiable account number – regard it as highly suspicious. Greetings like "Dear Lloyds Bank Customer" or "Dear eBay User" suggest that the sender is trying to catch anyone who happens to receive the mail, and they have no idea who you are or whether you really do have an account or business relationship with Lloyds or eBay. If the identifier is one of your email addresses (e.g. "Dear henry056@hotmail. com", that is *equally* suspicious. It's trivial to insert the email address into the message, and you should assume that it is not genuine.
- However, if it *does* include your real name, that isn't a *guarantee* that it's genuine. There are many ways of obtaining that information. In fact, sometimes it can be harvested from your full email identifier, without any need to find it out from other sources. If you do have an identifier, especially a numeric or alphanumeric identifier – and if you don't have such an identifier, maybe you shouldn't be using the service – you should check it. For instance, it's common for eBay phishes to include tags like "Your registered name is included to show that this message came from eBay," without actually showing the registered name, or it might even use a made-up identifier in the hope that you won't notice.
- Reading message headers is a dark art requiring years of study at Hogwarts. Well, not really. But many people are intimidated by it. However, here are a couple of things to watch out for, that don't require you to read the full headers.
    - If the mail doesn't seem to be addressed to anyone, it was blind copied to you and, probably, any number of other people. Don't trust it.
    - It may seem to be addressed to someone else, including the apparent sender of the mail, or to a generic name such as "customer" or "clientlist." This is sometimes appropriate for mail sent to many people, especially if the blind copy field is used to preserve their privacy. However, where the message concerns sensitive information such as banking data, it shows an inappropriate lack of personalization.
- If you receive email apparently from an institution with which you have a business relationship (say eBay, or a tax office) that doesn't mean that

you should accept it unquestioningly. If the message requires you to authenticate yourself to a web site and it's not the sort of mail you'd *expect* to get from them, it's suspicious. Security warnings are actually particularly suspicious: email advising you that your account has been compromised is a common phish type. A telephone notification can also be malicious, but it may be easier to ascertain whether it's genuine: at any rate, it can't be purely random, and there are ways of verifying such as calling back a known valid number (for instance, the number found on an account statement).

- Even if you are reasonably sure that the mail is genuine, do *not* click on an embedded URL directing you to a login page. If you have a pre-existing relationship with the organization, for instance if you already do e-Banking with them, you should already have a standard login procedure: use that rather than responding to a possibly-random email. If you need to contact them by phone, avoid using phone numbers included in the message. Just as web sites can be spoofed, so can telephone numbers. use the telephone directory or another trustworthy resource such as an account statement.
- A particularly common trick (but also a clear indication of mischief if you spot it) is an embedded URL that looks legitimate but has been modified to hide the real target. URLs can be obscured in many ways. However, if inspecting the source code for HTML mail or even passing the cursor over the URL shows a mismatch between the apparent site name and the target URL the browser actually sees, this is very suspicious. For example:
    - Deceptive text inserted between http:// and an "@" symbol: this may include the apparent target name, but will be ignored by the browser, which will only interpret the text that follows the @ as the domain name.
    - The domain name may be expressed as an IP address in one of several formats (dotted-decimal, dword, hexadecimal or octal). The characters forming the URL may also be expressed as hex: there are some examples at http://www.pc-help.Org/obscure.htm.
    - The URL may be made so long that it cannot be completely displayed in the status bar.
    - The URL may include a domain name that is not quite the same as the company's real domain, but is similar enough to evade a cursory glance.
- One of the weapons in the phisher's armoury is to present the 'problem' that requires you to log in as requiring urgent resolution ("You must log in within 24 hours or your account will be terminated for security reasons.") This variation on a well-known sales technique ("Offer only lasts till the end of today!") is intended to panic you into responding.
- Apart from increasing the pressure on the victim, it also works to the advantage of the phisher, who often needs an urgent response before law enforcement and other countermeasures are put into place.

The kind of crude, text-only phish (usually written in bad English) that we saw a few years ago is far rarer today, but the basic form of the attack hasn't changed

much: only the quality of the social engineering and the far more professional presentation.

However, the attack surface and range of vectors have broadened considerably: whereas most phishing attacks used to be delivered through email, we now see other forms of messaging exploited, such as SMS (texting), social media like Facebook and Twitter, even voicemail. And whereas phishing-related malware is still mostly Windows targeting, attacks that rely purely on social engineering and fake web sites might be delivered by any platform, including smartphones and tablets.

Finally, here are a few relevant resources from ESET:

- ESET white paper on spams and scams: The Spam-ish Inquisition
- ESET white paper on Phishing: A Pretty Kettle of Phish
- ESET Conference paper on phishing quizzes and educational measures: Phish Phodder: Is User Education Helping or Hindering?
- Phish-related ESET blogs: http://blog.eset.com/?s=phishing