

Beware of phishing-!

... don't bite the baited hook-!

Definition



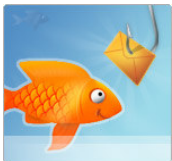
(fish´ing) (n.) The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information. [...]

(source : <http://www.webopedia.com>)

Explanation-:

Scammers are becoming increasingly more present on the world wide web. Some of their fraudulent attempts are very obvious, especially when you have heard about them at least once. But newbies are easy prey. This is why we thought it could be worth writing an article about this.

Phishing is easy to understand. Even if it takes on many different aspects, they all are basically the same. Indeed, phishing mainly consists of getting in touch with the victim either by email or via a fake website and pretend you represent an honest and official organization. What scammers are targeting is always the same : your money.



Most of the time, scammers will try to convince you to do what they want in order to get your money thanks to very appealing arguments. This is why there are many ways of doing this.

Phishing attempts are often done randomly. Email addresses can be harvested very easily on the website. Consequently, from time to time you will receive an email from someone or some organization you have never heard about and you will just report it as a spam. But sometimes, they will talk about something you know or propose something you want, something very appealing. This is where it really starts.

Examples :

1. The following example is very frequent on auction websites. Let's us pretend you are selling an item, an expensive one. The scammer will contact you and ask you to send it quickly. What they do is propose electronic payment methods, sometimes unknown, sometimes well-known. They send the money, you can see that your account has been credited with the money and you send the item right away as requested. The reason why they ask you to send the item quickly is simple : their payment was fake and the money is soon withdrawn from your account. The best thing to do in such a case is to wait at least 24 hours and see what happens. Of course only do this if you have doubts because it would contrast with the advantage of electronic payment methods, namely their rapidity.
2. This example is pretty much like the first one but this time, scammers are using a third party. They say the money is sent to a third party company. You receive a confirmation from this company which tells you that the money will be transferred to your bank account when the buyer receives the item. Of course, you never receive the money. Such third party companies do exist and we recommend using them when a considerable amount of money is at stake. Therefore, if you have doubts, do not hesitate to carry out an investigation and ask others for help.
3. In addition to the first 2 examples, it is important to say that sometimes, scammers do not hesitate to meet you personally. In this case, what they give you is a fake check. They even pretend to be giving you more money than asked so the whole deal seems even more appealing.
4. You receive an email from a website you already know asking you to update your personal info because, for instance, your credit card number is not valid anymore. The link provided in the email takes you to a fake website which looks exactly alike the real one. Therefore, when you try to log in, what you actually do is give the scammers the key to your account on the real website. No need to explain why.
5. Scammers will ask you if they can transfer a considerable amount of money to your account. The reasons can be very different but the bait they are using is once more very appealing. Let's pretend they want to transfer \$1000 to your account for any reason. What they do for such a favor, before asking you to transfer the money back to another account, is suggest you to keep part of it, let's say \$100. But a little while after having transferred money to another bank account, your bank tells you that the deposit had to be cancelled because somehow it is not valid. Do the math, you end up losing \$900.



Solutions :

1. Be careful and examine every golden opportunity ! Each time you have doubts (website address, IP address, contact, reason, ...), carry out an investigation!
2. Many websites (Delcampe.net is one of them), have very useful tools to download for free, which help you to know if you are on a real or a fake website. By downloading the Delcampe Toolbar (here), you will be able to do so. If the light is green, this means you are on the right website. 🟢
3. Read feedbacks carefully and wisely!
4. Share this article with as many Internet users as you can!

Helpful links:

<http://www.commentcamarche.net/attaques/phishing.php3>

<http://www.hoaxbuster.com/>

<http://www.hoaxbuster.com/hoaxliste/hoax.php?idArticle=22498>

<http://www.antiphishing.org/>

(English)

<http://www.vnunet.fr/actualite/securite/protections/20051018010>

(articles)

<http://www.generation-nt.com/actualites/9788/Disponibilite-de-l-anti-phishing-de-Microsoft>

(Microsoft tool)

<http://www.delcampe.com/toolbar.php?language=F>

(Delcampe Toolbar)

http://www.pcinpact.com/actu/news/Phishing_sous_Paypal_le_leurre_et_largent_du_leurr.htm

(Examples)

<http://www.sophos.fr/spaminfo/bestpractice/phishing.html>

(advice)

<http://www.p-p-p-powerbook.com/>

(fun)

<http://www.newtimes-slo.com/archive/2003-12-17/cover/>

(no comment)

<http://www.infobel.com/france/>

<http://www.infobel.com/france/wp/revsearch/default.asp>

http://www.whitepages.com/10001/reverse_phone

<http://www.whitepages.com/>

(white pages and reverse phone to check truthfulness of phone numbers and addresses)