

Introdução

Alguns utilizadores dentro do universos dos nossos Clientes, continuam a ser objecto do envio mais ou menos sistemático de emails com informação não solicitada.

Tal pratica, vulgarmente conhecida como "spam", não é possível de evitar completamente, até por ser impossível impedir seja quem for de enviar emails para um determinado endereço.

Os problemas causados pelo spam podem ser contrariados através de serviços quer internos (firewall), quer externos (no próprio provider) que assinalem e detectem os e-mail que são spam. Este tipo de soluções, não sendo eficaz a 100% o problema (visto que há sempre um certo numero de e-mail que não é possível detectar automaticamente como spam) permite minorar muito o problema.

Spam

Apesar de todos os filtros e protecções existentes, pode acontecer que os utilizadores de um sistema informático recebam emails não solicitados, quer de divulgação de publicidade não solicitada (spam).

Este tipo de actuação, cuja principal consequência é atulhar as caixas de correio com emails inúteis que é necessário apagar (com a consequente perda de tempo) sóp pode na pratica ser contrariado com a utilização de ferramenteas que bloqueiam este tipo de mensagens.

Phishing

Muito mais grave do que anterior é a recepção de emails igualmente não solicitados contendo quer de pedido de informações pessoais, financeiras, bancárias, ou de cartões de credito.

O que é o phishing?

Em computação, phishing é uma forma de "Engenharia Social", caracterizada por tentativas de adquirir informações sensíveis, tais como senhas e números de cartão de crédito, fazendo-se passar, quem o origina, por uma entidade credível, através do envio de um e-mail ou uma mensagem instantânea. O termo Phishing surge das cada vez mais sofisticadas artimanhas para "pescar" (fish) as informações sensíveis dos utilizadores.

Quais são os perigos do phishing?

São todos os que podem advir da utilização fraudulenta de elementos bancários (nomeadamente utilização fraudulenta de cartões de credito) ou de serem praticados em nosso nome actos ilícitos (roubo de identidade)

Como funciona o phishing?

Para que o phishing funcione, o autor mal-intencionado envia milhões de emails falsos que parecem vir de sites populares ou credíveis, como o seu banco ou empresa de cartão de credito. Esses emails, e os sites a que remetem, parecem oficiais o suficiente para convencer

muitas pessoas de sua legitimidade. Acreditando que esses emails são autênticos, pessoas desavisadas com frequência respondem às solicitações de número do cartão de crédito, senha, informações de conta ou outras informações pessoais.

Para fazer com que esses emails pareçam ainda mais reais, os criadores de "scam" podem colocar um link em um e-mail falso que parece levar ao site legítimo, mas na verdade leva o utilizador ao site de fraude ou mesmo a uma janela pop-up igual à do site oficial. Uma vez entrado num desses sites, o utilizador poderá, inadvertidamente, inserir informações pessoais, que serão transmitidas directamente ao criador do site, que por sua vez poderá usar esses dados para comprar bens, candidatar-se a um novo cartão de crédito ou roubar a identidade.

Como é que os piratas sabem o meu email?

A captura de emails é normalmente feita quer por testes massivos de envio de emails, quer por scanning de mensagens colocadas em forums ou blogs, quer ainda por "spyware" ou "chain letters". O ataque pode ser direccionado quer aos computadores do próprio utilizador, quer a quaisquer outros PC's onde eventualmente os emails constem.

Como lidar com um email que pode ser uma tentativa de phishing?

O principal conselho é de que nunca se deve responder a um e-mail que se suspeite, ainda que remotamente, possa ter estas características. De igual modo não devem ser seguidos quaisquer links que nos mesmos possam ser indicados. A ocorrência de phishing deve ser reportada ao Gestor do Sistema Informático.

Para uma informação o mais completa sobre este assunto, abaixo transcrevemos:

· Watch out for " phishy" emails. The most common form of phishing is emails pretending to be from a legitimate retailer, bank, organization, or government agency. The sender asks to " confirm" your personal information for some made-up reason: your account is about to be closed, an order for something has been placed in your name, or your information has been lost because of a computer problem. Another tactic phishers use is to say they' re from the fraud departments of well-known companies and ask to verify your information because they suspect you may be a victim of identity theft! In one case, a phisher claimed to be from a state lottery commission and requested people' s banking information to deposit their " winnings" in their accounts.

· Don' t click on links within emails that ask for your personal information. Fraudsters use these links to lure people to phony Web sites that looks just like the real sites of the company, organization, or agency they' re impersonating. If you follow the instructions and enter your personal information on the Web site, you' ll deliver it directly into the hands of identity thieves. To check whether the message is really from the company or agency, call it directly or go to its Web site (use a search engine to find it).

· Beware of " pharming." In this latest version of online ID theft, a virus or malicious program is secretly planted in your computer and hijacks your Web browser. When you type in the address of a legitimate Web site, you' re taken to a fake copy of the site without realizing

it. Any personal information you provide at the phony site, such as your password or account number, can be stolen and fraudulently used.

- Never enter your personal information in a pop-up screen. Sometimes a phisher will direct you to a real company' s, organization' s, or agency' s Web site, but then an unauthorized pop-up screen created by the scammer will appear, with blanks in which to provide your personal information. If you fill it in, your information will go to the phisher. Legitimate companies, agencies and organizations don' t ask for personal information via pop-up screens. Install pop-up blocking software to help prevent this type of phishing attack.

- Protect your computer with spam filters, anti-virus and anti-spyware software, and a firewall, and keep them up to date. A spam filter can help reduce the number of phishing emails you get. Anti-virus software, which scans incoming messages for troublesome files, and anti-spyware software, which looks for programs that have been installed on your computer and track your online activities without your knowledge, can protect you against pharming and other techniques that phishers use. Firewalls prevent hackers and unauthorized communications from entering your computer – which is especially important if you have a broadband connection because your computer is open to the Internet whenever it' s turned on. Look for programs that offer automatic updates and take advantage of free patches that manufacturers offer to fix newly discovered problems. Go to www.onguardonline.gov and www.staysafeonline.org to learn more about how to keep your computer secure.

- Only open email attachments if you' re expecting them and know what they contain. Even if the messages look like they came from people you know, they could be from scammers and contain programs that will steal your personal information.

- Know that phishing can also happen by phone. You may get a call from someone pretending to be from a company or government agency, making the same kinds of false claims and asking for your personal information.

- If someone contacts you and says you' ve been a victim of fraud, verify the person' s identity before you provide any personal information. Legitimate credit card issuers and other companies may contact you if there is an unusual pattern indicating that someone else might be using one of your accounts. But usually they only ask if you made particular transactions; they don' t request your account number or other personal information. Law enforcement agencies might also contact you if you' ve been the victim of fraud. To be on the safe side, ask for the person' s name, the name of the agency or company, the telephone number, and the address. Get the main number from the phone book, the Internet, or directory assistance, then call to find out if the person is legitimate.

- Job seekers should also be careful. Some phishers target people who list themselves on job search sites. Pretending to be potential employers, they ask for your social security number and other personal information. Follow the advice above and verify the person' s identity before providing any personal information.

· Be suspicious if someone contacts you unexpectedly and asks for your personal information. It's hard to tell whether something is legitimate by looking at an email or a Web site, or talking to someone on the phone. But if you're contacted out of the blue and asked for your personal information, it's a warning sign that something is "phishy." Legitimate companies and agencies don't operate that way.

· Act immediately if you've been hooked by a phisher. If you provided account numbers, PINS, or passwords to a phisher, notify the companies with whom you have the accounts right away. For information about how to put a "fraud alert" on your files at the credit reporting bureaus and other advice for ID theft victims, contact the Federal Trade Commission's ID Theft Clearinghouse, www.consumer.gov/idtheft or 877-438-4338, TDD 202-326-2502.

· Report phishing, whether you're a victim or not. Tell the company or agency that the phisher was impersonating. You can also report the problem to law enforcement agencies through the National Fraud Information Center/Internet Fraud Watch, www.fraud.org or 800-876-7060, TDD 202-835-0778. The information you provide helps to stop identity theft.