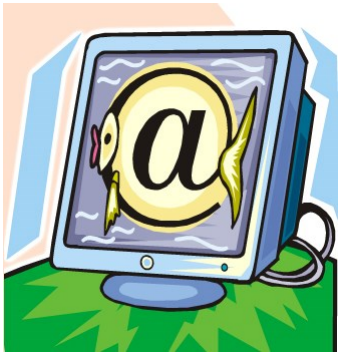
O que é o Phishing?



O “phishing” (trocadilho com "fishing", ou “ir à pesca” em inglês, dado que a informação é como que um “anzol” que se espera que alguém “morda”) consiste em utilizar métodos vários que levem o utilizador a revelar dados pessoais e confidenciais, como os seus números de cartão de crédito, informação de contas bancárias, números de segurança social, palavras-chave e outros.

REFERÊNCIA BIBLIOGRÁFICA

SeguraNet - *O phishing*. [Em linha]. [Consult.17 de Janeiro de 2011]. Disponível em: WWW:<URL: http://www.seguranet.pt/educadores/>.

ESCOLA SECUNDÁRIA DR. JOAQUIM DE CARVALHO, FIGUEIRA DA FOZ

BIBLIOTECA ESCOLAR

BLOGUE: http://www.netbiblio.blogspot.com

E-mail: biblioteca@esjcff.pt

Escola Secundária Dr. Joaquim de Carvalho, Figueira da Foz
Biblioteca Escolar

Guia

SeguraNet

Phishing

Phishing

Como funciona o Phishing?

Os “phishers” recorrem a várias formas de obtenção de informação, nomeadamente, SPAM, mensagens de pop-up ou e-mails, fazendo-se passar por empresas ou organizações legítimas com as quais, a potencial vítima tem negócios - por exemplo, o seu fornecedor de serviços de Internet (vulgo ISP), o banco, os serviços de pagamentos on-line ou até um organismo governamental.

Estas mensagens costumam alegar que o utilizador precisa de “actualizar” ou “validar” a informação da sua conta, chegando a ameaçar com consequências negativas (o fecho da conta, por exemplo) caso não haja resposta.

A estas técnicas de ameaça e manipulação dá-se o nome de Engenharia Social, nas quais também se inserem as formas mais sedutoras de persuasão, como a “oferta” de artigos, viagens ou dinheiro, por Internet.

Que perigos pode apresentar o Phishing?

A mensagem maliciosa que foi enviada pode reencaminhar a pessoa para um sítio de Internet que parece legítimo mas, na verdade, não é. O propósito deste sítio fraudulento é convencê-la a divulgar informação pessoal que permita aos burlões roubar-lhe a sua identidade e debitar contas ou cometer crimes em seu nome.

Outras formas de phishing envolvem subterfúgios técnicos e têm como objectivo inserir um programa malicioso no seu computador que irá obter e enviar, os dados pretendidos, aos seus autores.

Que cuidados ter?

Pode seguir algumas orientações que eventualmente ajudem a evitar um logro, por este tipo de fraudes:

• Se receber um e-mail ou pop-up que lhe peça informação pessoal ou financeira, não responda nem clique no link da mensagem.

• Lembre-se: empresas legítimas não pedem este tipo de informação por correio electrónico
Se está preocupado com a sua conta ou se tem dúvidas quanto ao remetente ou conteúdo da mensagem, entre em contacto com a organização (alegada autora da mensagem) através de um número de telefone que sabe ser legítimo, ou abra uma nova sessão no Browser e aceda ao endereço correcto da empresa. Em qualquer caso, não copie o link da mensagem.

• Não envie informações pessoais ou financeiras, por e-mail
O e-mail não é um método seguro para transmissão de informações pessoais. Se iniciou uma transacção através de um sítio de Internet e deseja fornecer dados pessoais ou financeiros através desse sítio, procure indicadores de que o mesmo é seguro, tal como um ícone de um cadeado na barra de status do browser ou um URL que comece com "https:" (o "s" significa "secure"). Infelizmente, nenhum indicador é à prova de falhas; alguns "phishers" já falsificaram ícones de segurança.

• Veja regularmente os extractos do seu cartão de crédito e contas bancárias para determinar se há débitos indevidos
De preferência, verifique-os assim que os receber. Se estes extractos se atrasarem mais do que um par de dias, telefone ao seu banco e solicite essa informação.

• Use software antivírus e mantenha-o actualizado
Alguns e-mails de phishing contêm software que pode causar danos no seu computador ou monitorizar as suas actividades na Internet sem o seu conhecimento. Um antivírus e uma firewall podem protegê-lo de aceitar, inadvertidamente, esse tipo de ficheiros.

O software antivírus verifica as comunicações recebidas, procurando detectar ficheiros problemáticos. Uma firewall ajuda a torná-lo “invisível”, na Internet, e bloqueia todas as comunicações de fontes não autorizadas. É particularmente importante ter uma firewall se tem uma ligação de banda larga.

Além de tudo isto, o seu sistema operativo (tal como Windows ou Linux) pode disponibilizar "patches" gratuitos de software para fechar "buracos" de segurança que hackers ou phishers viessem a explorar.

• Seja cuidadoso quando abrir qualquer anexo ou descarregar quaisquer ficheiros a partir de e-mails que receba, independentemente do remetente
Não se esqueça que há vírus que enviam e-mails através de remetentes familiares. O facto de ter o seu computador livre de vírus não implica que os seus amigos e contactos, no mundo virtual, também estejam na mesma situação.