internet segura.pt

"PESCAR" DADOS ONLINE NÃO DEIXES QUE APANHEM OS TEUS!

O roubo de dados pessoais é um dos crimes mais praticados na Internet. São várias as formas através das quais os criminosos tentam "pescar" os nossos dados. Para que nunca mordas o "anzol", ensinamos-te quais as técnicas mais populares para roubar dados:

PHISHING

O phishing é um tipo de roubo de identidade online. Utiliza o correio eletrónico e/ou websites/links fraudulentos concebidos para roubar os teus dados ou informações pessoais, como números de cartões de crédito, palavras-passe, dados de contas ou outras informações. Este termo deriva do inglês "fishing" – pescar – uma vez que estes grupos lançam o anzol e fazem-se passar por entidades geralmente conhecidas e credíveis, para obter acesso a contas privadas. Os criminosos podem depois utilizar estas informações para vários tipos de fraude, como roubar dinheiro da tua conta, abrir novas contas em teu nome, obter documentos oficiais utilizando a tua identidade, fazer ataques informáticos ou praticar cyberbullying em teu nome.

SMISHING

É uma forma de phishing que se baseia no envio de uma mensagem de telemóvel (SMS ou MMS) que procuram direcionar o destinatário da mensagem de texto para visitar um website ou ligar para um número de telefone, que procura seduzir a pessoa para fornecer informações confidenciais, como detalhes de cartão de crédito, senhas ou outra informação pessoal. Pode acontecer que por responder à mensagem, o recetor vê confirmado um vínculo a um serviço que vai cobrar uma quantia diária. Os websites de smishing sites também são conhecidos para tentar infetar o computador ou smartphone do recetor da mensagem.

VISHING

O termo vishing combina os termos voz e phishing. Os criminosos também podem utilizar serviços como o Skype ou a telefonia móvel para enganar as pessoas. Um e-mail aparentando ser de uma instituição totalmente legítima, convida o recetor a contactar a entidade por telefone. No momento da chamada, o recetor da mensagem não é atendido por uma pessoa, mas sim por um atendedor automático, que solicita vários dados pessoais para "verificação de segurança".

SPEAR-PHISHING

Neste caso, um e-mail é enviado por alguém que se faz passar por uma pessoa conhecida. O sucesso deste esquema deve-se ao uso de expressões familiares como fosse alguém dos nossos contactos "olá João, estás bom?". O objetivo é fazer com que o recetor da mensagem acredite que os ficheiros ou links enviados no e-mail provêm de alguém que conhece, para assim não ter problemas de os abrir e acabar por dar acesso aos seus dados pessoais ou ao controlo do seu computador.

Queres saber mais? Vai a www.internetsegura.pt ou www.facebook.com/internetsegura.pt e consulta tudo sobre este e outros temas. Navega em segurança!

LINHA AJUDA
internet segura.pt
808 91 90 90

Linha Alerta
internet segura.pt
linhaalerta.internetsegura.pt

ALGUMAS DAS BURLAS QUE CONTINUAM A CIRCULAR

A RAPARIGA RUSSA

Uma jovem encontra "por acaso" o endereço de e-mail do utilizador, mostrando interesse em conhecê-lo pessoalmente. Os e-mails continuam tentando seduzir a vítima. Após se declarar apaixonada pelo utilizador, pede a este algum dinheiro para comprar bilhetes, tratar de vistos e burocracias (cerca de mil euros também). Após a transferência desta quantia, a rapariga desaparece.

OFERTAS DE EMPREGO

Uma companhia estrangeira diz estar a recrutar agentes financeiros, tratando-se de um trabalho possível de ser realizado a partir de casa, e dando acesso a cerca de três mil euros em troca de quatro horas de trabalho por dia. Ao aceitar as condições, são solicitados os dados bancários do utilizador. A vítima passará a receber dinheiro roubado de outras contas bancárias que deverá transferir conforme solicitado. No caso de existir uma investigação, o utilizador será considerado cúmplice.

HOTMAIL/FACEBOOK

Este esquema está a tornar-se cada vez mais popular. Os cibercriminosos modificam as passwords das contas de e-mail ou Facebook da vítima, para impedirem que esta aceda à sua conta. Entretanto, é enviada uma mensagem a todos os contactos do utilizador, informando que se encontra de férias e que foi roubado. Por esse motivo, pede aos contactos para lhe transferirem quantias que variam entre os quinhentos e os mil euros para pagar o hotel e/ou viagem.

5 DICAS PARA TE PROTEGERES DESTAS FRAUDES

#1 Tem um antivírus atualizado e ativa o antispam da tua caixa de correio - grande parte destas mensagens serão detetadas e classificadas como indesejadas por estas soluções de segurança;

#2 Nunca divulgues passwords ou forneças dados pessoais a ninguém;

#3 Não abras anexos ou links de destinatários desconhecidos e lê os endereços de e-mail para teres a certeza de que foram mesmo enviados pelos teus amigos;

#4 Não respondas a chamadas ou SMS de números anónimos ou desconhecidos;

#5 O bom senso é o teu melhor aliado para evitar fraudes.

E já sabes: se tiveres algum problema, informa-te junto do Centro Internet Segura.