manchete

Jornal Negócios
Investidor Privado
03-01-2017

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 18239

Temática: Sociedade
Dimensão: 2385 cm²
Imagem: S/Cor
Página (s): 2 e 3

As armas para se defender das fraudes na internet

RUI BARROSO
ruibarroso@negocios.pt
CÁTIA SANTOS
Ilustração

É um dos tipos de criminalidade que mais cresce e com tácticas cada vez mais complexas. Mas há formas de minimizar o risco de ser apanhado pelos cibercriminosos.

Portugal é um dos países em que o risco de ser vítima de software malicioso é mais elevado. Mas há formas de minimizar o risco de ter o computador ou 'smartphone' arrombado. Todos os cuidados são poucos numa altura em que a criminalidade na internet não pára de crescer.

Os crimes que mais aumentam em Portugal são as extorsões (principalmente através da internet) e a burla informática, com subidas de 70% e 20%, segundo o relatório de análise da criminalidade participada até ao terceiro trimestre de 2016, citado pelo Diário de Notícias.

Além do crescimento deste tipo de crimes, Portugal é um dos países em que existe maior probabilidade de infecções online, segundo a empresa de cibersegurança Kaspersky. O risco é de 35%, o 12º mais elevado do "ranking" elaborado por esta firma. As ameaças são muitas. E as formas de protecção também.

"Como existem vários ilícitos que podem ser classificados de burla informática, as recomendações acabam por ser também muito variadas", refere Pedro Veiga, coordenador do Centro Nacional de Cibersegurança (CNCS), ao Negócios.

O responsável desta entidade revela que "o CNCS continua a receber notificações de casos relacionados com furto de identidade e observamos um crescimento no número de casos de 'ransomware', estes últimos num crescendo de complexidade e impacto". Neste último caso, através da instalação de "softwares" maliciosos impede-se que o utilizador tenha acesso aos seus próprios ficheiros, sendo exigida uma compensação, muitas vezes financeira, para resgatar esses ficheiros.

E este tipo de crime tem-se generalizado a nível global. A Kaspersky refere mesmo que "2016 pode ser declarado o ano do 'ransomware'". E a empresa alerta que começam a ser cada vez mais frequentes os casos em que após o pagamento do resgate, a informação que foi feita refém não é libertada.

Uma das portas de entrada para "ransomware" e de outros tipos de "malware" é o correio electrónico. E uma das recomendações deixadas por Pedro Veiga é de se estar atento "à origem das mensagens". Realça que "ainda que conheçamos a pessoa que supostamente enviou a mensagem, devemos sempre questionar a sua autenticidade e questionar o remetente telefonicamente se enviou realmente aquela mensagem".

Além do "ransomware", outros dos ilícitos mais comuns são o furto de identidade. Neste aspecto , o coordenador do CNCS refere que "se a burla envolver algum tipo de identidade digital ou credenciais de acesso a serviços on-line, deverá proceder à sua revogação ou alteração imediatas". E recomenda criar passwords seguras.

"Ransomware" e furto de identidade são dos crimes informáticos mais comuns em Portugal.

Com tantas formas de os cibercriminosos entrarem em aparelhos informáticos alheios, "não existe dispositivo de segurança no mundo que consiga proteger contra todas as ameaças possíveis", refere a empresa de cibersegurança Sophos. Mas há pequenos passos que podem ser dados para diminuir os riscos e colocar algumas trancas nas entradas dos dispositivos informáticos. No entanto, se mesmo assim, as portas forem arrombadas, a primeira coisa a fazer é "participar a ocorrência à polícia mais próxima", conclui Pedro Veiga. ■

manchete

Jornal Negócios
Investidor Privado
03-01-2017

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 18239
Temática: Sociedade
Dimensão: 2385 cm²
Imagem: S/Cor
Página (s): 2 e 3

OS CUIDADOS A TER PARA SE PROTEGER DOS CIBERCRIMINOSOS

O leque de crimes na internet é cada vez maior e com recurso a tácticas mais sofisticadas. Confira os passos a seguir para se proteger do cibercrime.

Os "raptos" e as extorsões via internet

O "ransomware" é um dos crimes informáticos que mais tem crescido. Através de softwares maliciosos, os cibercriminosos encritpam ficheiros impedindo que a vítima tenha acesso à informação do dispositivo infectado ou até ao próprio aparelho. Para libertar os ficheiros exigem o pagamento de um resgate, muitas vezes através de "bitcoins". Mas sem garantias de que o pagamento resolva o problema ou que no futuro não existam novos sequestros. Apesar de não haver formas 100% eficazes de impedir estes sequestros, ter programas antivírus e antimalware actualizados pode ajudar a diminuir o risco. Outro dos cuidados a ter é evitar fazer "downloads" de sites que possam ter problemas de segurança e evitar abrir anexos nos emails de fontes desconhecidas. Ao detectar que se foi vítima de "ransomware", o melhor é desligar o aparelho da rede em que está inserido e contactar as autoridades. ■

Os cuidados com o email e com as passwords

Emails e passwords devem ser alvos de cuidados especiais. "Devemos estar atentos à origem das mensagens e ainda que conheçamos a pessoa que supostamente enviou a mensagem, devemos sempre questionar a sua autenticidade", refere o Centro Nacional de Cibersegurança (CNCS). E recomenda "apagar de imediato mensagens cuja origem não conhecemos e não seguir ligações duvidosas". Também as passwords devem ser alvo de cuidados especiais. "Crie passwords seguras, incluindo letras maiúsculas e minúsculas, números e outros caracteres especiais. Utilize passwords distintas e mais complexas de acordo com a importância do site e da informação nele tratada", refere o CNCS. E dá mais alguns conselhos: "Não use nomes comuns como a sua equipa favorita, os artistas do momento e, especialmente, nunca divulgue a password se lhe telefonarem para casa". ■

Quando a esmola é muita, é de desconfiar

Fazer compras e vendas online é algo que também exige atenção redobrada para evitar ser alvo de burla. "Nos sites de venda online devemos desconfiar dos produtos demasiado baratos ou cuja origem não é confiável, onde o vendedor não tem uma morada postal credível ou afirma estar em localizações invulgares", recomenda Pedro Veiga, coordenador do CNCS. Acrescenta que "devemos escolher sites que disponibilizam mecanismos de avaliação por pares e evitar sempre que possível vendedores muito recentes". Também nestes sites, Pedro Veiga diz que se deve evitar "fornecer o número de cartão de crédito ou quaisquer identificadores pessoais tais como telefone ou morada e verifique se é usado um protocolo seguro [com https:// na barra de endereços]". No caso da compra ser feita depois de forma presencial, é aconselhável escolher um local movimentado e não ir sozinho. ■

Escapar aos furtos de indentidade

O furto de identidade continua a ser um dos tipos de criminalidade mais comuns. E as tentativas dos cibercriminosos acederem à informação pessoal podem vir de várias fontes. Desde falsos anúncios de emprego em que são solicitados dados pessoais, até à utilização de informações que se possam colocar nas redes sociais. Outra das formas de roubar dados pessoais é através do "phishing", que tende a ser direccionado para se obter dados para entrar em contas bancárias, com links que redireccionam para páginas falsas em que são solicitados dados. Além de aceder sempre directamente ao site do seu banco e de seguir as recomendações de segurança, Pedro Veiga refere que "os bancos nunca telefonam para casa das pessoas a pedir passwords. E nunca pedem mais do que dois ou três algarismos dos cartões matriz". Sempre que for solicitada mais informação é de desconfiar. ■

O que fazer se for vítima de cibercrime

Apesar de todos os cuidados que se possam ter, e que minimizam o risco de se ser vítima de cibercrime, não há formas 100% seguras de ficar a salvo. Caso seja um dos alvos uma das primeiras coisas a fazer é contactar as autoridades, diz Pedro Veiga. Já no caso de "a burla envolver algum tipo de identidade digital ou credenciais de acesso a serviços on-line, deverá proceder à sua revogação ou alteração imediatas". No caso de furtos de identidade que permitem ao cibercriminoso entrar nas suas contas bancárias além de cancelar essas contas e mudar os código de acessos, deve também solicitar os "formulários necessários para contestar que as acções levadas a cabo pelo criminoso tenham sido praticadas pela vítima", segundo informação da Associação Portuguesa de Apoio à Vítima (APAV), que tem um site sobre as recomendações para prevenir e lidar com o cibercrime. ■

O "rapto" de dados é um dos cibercrimes que mais tem crescido. A Kaspersky diz que 2016 foi o ano do "ransomware".

Certificar-se das origens das mensagens de correio electrónico e ter passwords seguras são passos essenciais.

Nos sites de vendas online é necessário analisar os registos dos vendedores e ter cuidados com os pontos de entrega.

Sempre que lhe pedirem dados desconfie. Os bancos, por exemplo, nunca telefonam ou mandam emails a pedir passwords.

Contactar as autoridades e revogar credenciais de acesso são passos a seguir depois de ser vítima de cibercrime.