NÃO TE DEIXES IR COM A MARÉ

SEGURANÇA DIGITAL

Riscos e Recomendações

ASF
AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

ÍNDICE

NÃO NAVEGUES POR MARES DESCONHECIDOS

Se não conheces a origem de uma mensagem, *e-mail* ou *link* não cliques, não respondas. Existem muitos tipos de **fraude digital** à espera que embarques nessa viagem.

#PHISHING

A fraude digital está cada vez mais sofisticada, o que nos obriga a ter cuidados redobrados quando adquirimos produtos ou serviços *online*.

Já recebeste na tua caixa de *e-mail* anexos ou URL's de remetentes desconhecidos? Já te enviaram *links* suspeitos pelo *WhatsApp*? Já recebeste um *sms* a dizer que tens uma encomenda à espera na alfândega, sem teres encomendado nada? Cuidado, pode ser ***phishing***!

O *phishing* é uma prática fraudulenta que consiste no envio de *e-mails*, mensagens (*smishing*), ou ainda na realização de telefonemas (*vishing*), com o objetivo de levar o utilizador a clicar em *links* inseguros ou anexos maliciosos e a facultar informações pessoais (por exemplo: dados bancários) por acreditar que quem o solicita é uma entidade legítima. Este tipo de fraude permite que *hackers* se apropriem de dados pessoais dos utilizadores para acederem posteriormente às suas contas.

AVISO À NAVEGAÇÃO

Não abras *e-mails*, nem cliques em ligações de fonte desconhecida ou duvidosa (ex.: *pop-ups*);

Não abras *links* que te tenham enviado por *sms* e cujo número e conteúdo desconheças;

Sempre que for necessário disponibilizar dados pessoais, seja num *website*, seja através de uma chamada, ou outro meio, assegura-te da legitimidade do outro interveniente e partilha apenas a informação estritamente necessária.

As armadilhas no digital não ficam por aqui. Há muitos outros tipos de fraude a que deves estar atento.

Já alguma vez acedeste a um *website* e verificaste que o endereço não corresponde exatamente ao do fornecedor do produto ou serviço (há uma letra diferente, por exemplo)? Cuidado, podes ter sido direcionado para um *website* falso e estar a ser vítima de ***pharming***!

O *pharming* é uma prática fraudulenta, tecnologicamente mais sofisticada que o *phishing*, que consiste na instalação de um vírus no computador ou dispositivo móvel que irá depois redirecionar o utilizador para páginas falsas. Assim, mesmo que o utilizador digite o *link* corretamente, esse vírus fará com que seja redirecionado, sem que se aperceba, para uma página falsa com o objetivo de capturar os seus dados pessoais.

AVISO À NAVEGAÇÃO

Verifica sempre o endereço eletrónico (URL) com atenção durante toda a tua navegação;

Privilegia escrever o URL na totalidade, ao invés de clicar em *links* por ser mais rápido;

Certifica-te de que visitas *websites* fidedignos (com indicação de HTTPS e cadeado);

Verifica a política de privacidade dos *websites* que visitas (por exemplo, se o vendedor está devidamente identificado, se disponibilizam contactos e informação sobre reclamações).

#SPYWARE

Já foste confrontado com um anúncio de uma aplicação muito útil para ti, mas não conseguiste perceber a identidade do fornecedor? Já descarregaste algum programa ou aplicação de fontes não oficiais? Aparecem *pop-ups* no teu computador com muita frequência? O funcionamento do teu computador está mais lento do que o normal? Cuidado, o teu dispositivo pode ter sido infetado por um ***spyware***!

O *spyware* é um *software* malicioso, que à semelhança do *pharming* se instala num computador ou dispositivo móvel, sem que o utilizador se aperceba, e que monitoriza e recolhe secretamente toda a sua atividade, incluindo as teclas em que carrega, conseguindo, assim, obter informações sobre os seus hábitos de navegação, bem como dados pessoais (por exemplo.: credenciais de acesso). Este tipo de *software* pode ser instalado nos nossos equipamentos através do simples *download* de uma aplicação ou ficheiro aparentemente inofensivos.

AVISO À NAVEGAÇÃO

Não faças *downloads* de fontes desconhecidas e garante que as APP's que descarregas, para além de serem oficiais, se encontram sempre atualizadas. Para facilitar, podes tornar essas atualizações automáticas;

Mantém o antivírus dos teus equipamentos atualizado;

Controla as permissões que dás às tuas aplicações, até porque muitas delas podem nem ser necessárias ao seu funcionamento (ex: câmara, contactos, galeria, etc.).

Não consegues fazer ou receber chamadas? Não consegues sequer ter acesso ao teu telemóvel? Cuidado, podes estar a ser vítima de **SIM *swapping***!

Na prática fraudulenta de SIM *swapping* um terceiro toma controlo do teu telemóvel ao ligar para a tua operadora e pedir a transferência do teu número de telemóvel para um novo cartão SIM, este último sob o controlo de *hackers*. Nestas situações os *hackers* conseguem fazer prova de que são a pessoa responsável pelo número de telemóvel em questão, sem o serem na verdade. Como é que o conseguem fazer? Através da recolha de dados pessoais que obtêm nas redes sociais (por exemplo.: nome, data de nascimento, número de telemóvel, *e-mail*...), através de práticas fraudulentas como o *phishing* ou ainda de falhas de segurança em sistemas informáticos.

AVISO À NAVEGAÇÃO

Tem atenção à informação que partilhas através das redes sociais. Quando disponibilizas informação como a tua data de nascimento, morada ou contactos telefónicos podes estar a facilitar o acesso de *hackers* às tuas contas;

Tem atenção aos comentários que fazes nas redes sociais e que podem revelar muito sobre a tua rotina diária (por exemplo.: locais que frequentas, compras que fazes, períodos de férias) facilitando, assim, o acesso a terceiros aos teus hábitos de consumo e ficando mais vulnerável a tentativas de fraude;

Verifica as tuas definições de privacidade nas redes sociais, pois podes ter o perfil público e não saber.

#SHOULDER SURFING

Quando fazes pagamentos com cartão multibanco em lojas físicas, ou fazes *login* nas *apps* do teu telemóvel em público, tens em atenção quem pode estar à tua volta a observar-te? Cuidado com a técnica de ***shoulder surfing***!

Shoulder surfing consiste em observar uma pessoa "por cima do ombro", quando esta insere credenciais de acesso ou dados pessoais num dispositivo (por exemplo.: telemóvel, computador, *tablet*). Esta técnica, que visa também atingir propósitos fraudulentos, não necessita de acontecer no ambiente digital, mas terá certamente as suas consequências nesse meio.

AVISO À NAVEGAÇÃO

Não acedas às tuas contas *online* ou faças pagamentos sem ter em atenção quem pode estar à tua volta a observar-te;

Não uses a mesma *password* para todas as tuas contas;

Privilegia a autenticação multifator no acesso às tuas contas, uma vez que dificulta o acesso de terceiros;

Não te esqueças de bloquear o computador sempre que estiveres num sítio público (ex.: biblioteca, sala de estudo) e te ausentares, mesmo que por pouco tempo.

Já te aconteceu estares com pouca bateria e ligares o teu telemóvel a um posto de carregamento USB público? Cuidado com a técnica de ***juice jacking***!

Ao utilizares estações de carregamento públicas para carregar os teus dispositivos (muito comuns nos aeroportos ou em hotéis, por exemplo) corres o risco de comprometer os teus equipamentos e dados pessoais. Estas estações de carregamento podem ter sido alteradas para introduzirem vírus nos teus equipamentos. Se tiveres mesmo de recorrer a esta forma de carregamento, adota medidas de segurança.

AVISO À NAVEGAÇÃO

Evita carregar os teus dispositivos móveis num posto de carregamento USB público;

Verifica se os teus equipamentos já incluem um modo seguro de carregamento, que impeça a transferência de dados quando ligados a uma entrada USB;

Opta por carregar os teus dispositivos através de uma *powerbank* ou em tomadas na parede, uma vez que não permitem a transferência de dados.

NEM TUDO O QUE VEM À REDE É PEIXE

Como já percebeste existem vários tipos de fraude digital.
Será que já consegues "pescar" uma situação de fraude
se alguma te cair na rede?

Existem alguns sinais que podem indicar que te encontras perante uma situação de fraude. Fica atento aos seguintes sinais:

MAY DAY

O preço a pagar é bom de mais para ser verdade?

O endereço de *e-mail* do remetente é duvidoso?

O *e-mail* ou mensagem que recebeste contém erros ortográficos?

O nome do anexo não coincide com o título do *e-mail*?

O conteúdo da mensagem que recebeste é muito vago?

Existe urgência para que adquiras o produto ou serviço que te foi apresentado?

Existe a promessa de vires a ter um grande lucro?

Recebeste uma mensagem nas redes sociais de alguém que não conheces, mas que partilha contigo uma história de vida comovente e te pede de seguida ajuda financeira?

É importante adotares determinados comportamentos quando decidires adquirir produtos ou serviços *online*.

AVISO À NAVEGAÇÃO

Se tens dúvidas acerca da identidade do vendedor ou do produto ou serviço que oferece, procura mais informação antes de avançares para a compra;

Desconfia de publicações de entidades ou pessoas que não conheces com anúncios de ofertas irresistíveis;

Lê as críticas e/ou comentários de outros utilizadores sobre aquele vendedor;

Se se tratar de um produto ou serviço financeiro, verifica se se trata de uma entidade autorizada a vender esse produto ou serviço. Podes encontrar informação sobre as entidades autorizadas a comercializar seguros e fundos de pensões em Portugal no site da ASF, em www.asf.com.pt.

Tem especial atenção à forma como efetuas o pagamento dos produtos ou serviços que adquires.

AVISO À NAVEGAÇÃO

Não faças pagamentos *online* através de redes *WiFi* públicas, pois corres o risco de os teus dados bancários poderem ficar comprometidos;

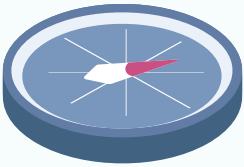
Privilegia o uso de cartões virtuais de utilização única ou com o saldo limitado ao valor que pretendes gastar;

Privilegia o uso de cartões com procedimentos de autenticação adicionais e verifica se os *websites* onde efetuas as tuas compras também dispõem de sistemas acrescidos de segurança (ex.: sistema *3D Secure*);

Quando fizeres um pagamento *online* escolhe entidades de pagamento legítimas e seguras (ex: Paypal);

Quando acedes ao *homebanking* nunca divulgues todas as coordenadas do teu cartão matriz;

Consulta periodicamente os movimentos da tua conta bancária.



NÃO PERCAS O NORTE.
HÁ BÚSSOLAS PARA TE ORIENTAR.

Se fores arrastado para uma situação fraudulenta
é importante saberes **como podes reagir**.

Compraste um produto *online* e ele nunca chegou?

Foste consultar os movimentos da tua conta e reparaste num pagamento que não autorizaste?

Agir rapidamente é muito importante em contextos de fraude digital. A denúncia deste tipo de situações a um órgão de polícia criminal (PSP, GNR ou PJ) ou ao Ministério Público revela-se fundamental para que possam ser desencadeados os procedimentos que permitam evitar novas situações de fraude.

Além da denúncia, é também essencial contactares de imediato o teu banco de modo a conseguir perceber-se a origem do movimento não autorizado e, se possível, prevenir prejuízos maiores.

AVISO À NAVEGAÇÃO

Se desconfiares que o teu cartão bancário possa ter sido comprometido pede que o mesmo seja bloqueado;

Se a situação o justificar, pede que os teus acessos ao *homebanking* sejam bloqueados;

Guarda sempre os comprovativos de todas as transações que efetuares e de outros elementos que possam ser usados como meio de prova (mensagens, cópias de anúncios, etc.);

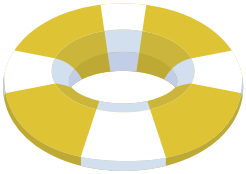
Não deixes de denunciar a situação. O que aconteceu contigo não tem de se repetir com outra pessoa.

Antes deste barco zarpar,

FICAM AQUI AS ÚLTIMAS DICAS

para uma navegação mais segura.

TODOS A BORDO!



- Cria palavras-passe fortes (que incluam, por exemplo, no mínimo 12 caracteres com maiúsculas, minúsculas, números e outros caracteres especiais (#, @) e que não contenham informação pessoal (ex.: nome próprio, data de nascimento, nome do teu animal de estimação…);

- Evita guardar as *passwords* no *browser*. Se possível, usa gestores de palavras-passe e altera-as com frequência;

- Não permitas que aplicações iniciem sessão automaticamente, sem que seja necessário fazer *login*;

- Não partilhes *passwords* com outras pessoas e não as guardes em sítios de fácil acesso (como numa agenda pessoal, em *post-its* ou no telemóvel);

- Altera o nome e a palavra-passe de origem da tua *WiFi* doméstica;

- Evita usar redes *WiFi* públicas, pois há um risco maior de comprometeres os teus dados pessoais;

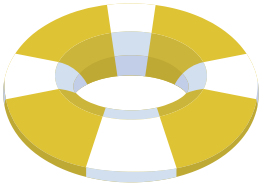
- Tapa a câmara e desliga o microfone do teu dispositivo quando não os estás a utilizar. Há vírus informáticos que conseguem ativar essas funcionalidades sem serem detetados;

- Evita ter a localização e o *Bluetooth* ligados quando já não os estás a utilizar;

- Evita carregar os teus dispositivos móveis num posto de carregamento USB público, pois os teus dados podem ser expostos se o mesmo tiver sido afetado com algum *malware*. Muitos equipamentos (*smartphones*, *tablets*, etc.) incluem um modo seguro de carregamento ou acesso a uma tomada USB para evitar a transferência de dados e proteger a ligação;

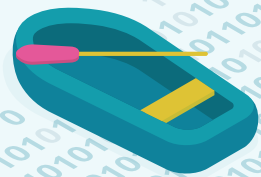
- Não insiras nos teus dispositivos, *pens* USB desconhecidas;

- Não cedas os teus equipamentos a outras pessoas sem supervisão.



A Internet está na crista da onda.
A fraude digital também!

NÃO TE DEIXES
IR COM A MARÉ



asf.com.pt