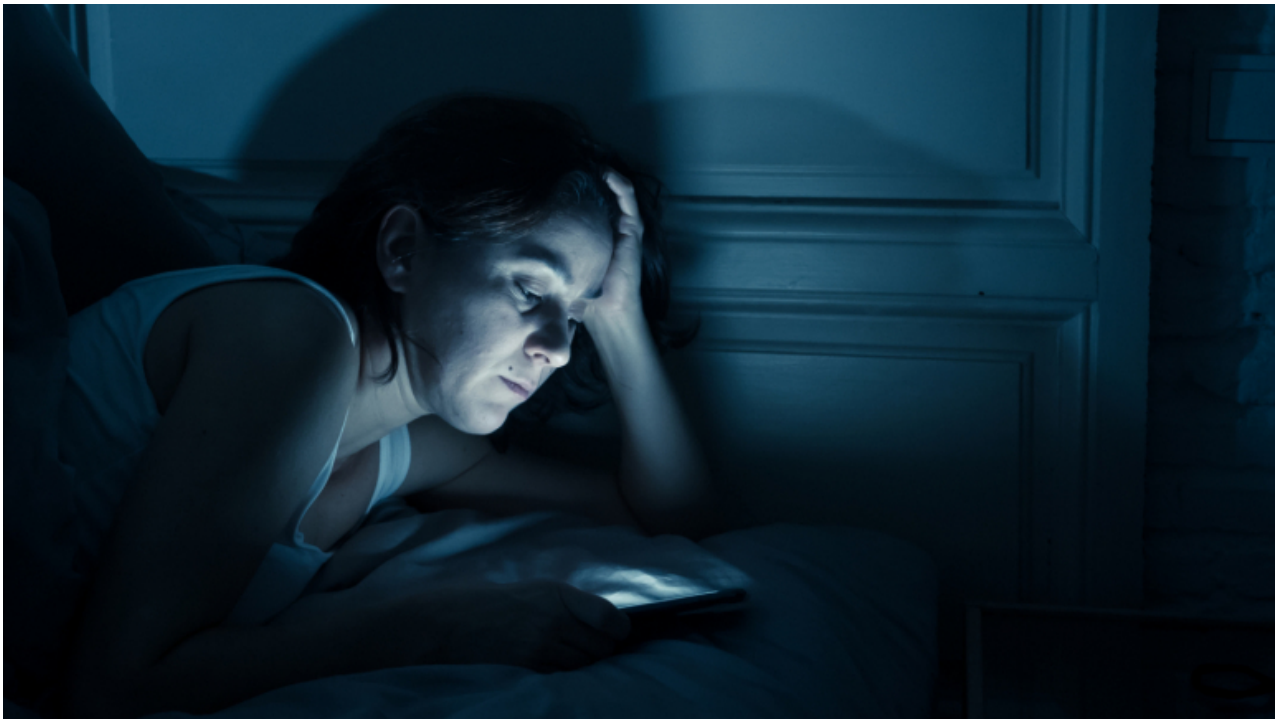
Está a passar mais tempo online? Deixamos dicas para o fazer em cibersegurança

observador.pt/2020/03/18/esta-a-passar-mais-tempo-online-deixamos-dicas-para-o-fazer-em-ciberseguranca/amp



Em fase de quarentena ou de isolamento, há um recurso que está a mostrar mais do que nunca para o que é que serve: a internet. Seja para trabalhar remotamente, para fazer partilhas nas redes sociais ou para comprar produtos em supermercados online há vários cuidados que é preciso ter. O importante é que se mantenha, de qualquer forma, em segurança.

A Polícia Judiciária, o Centro Nacional de Cibersegurança e os especialistas em segurança informática têm deixado, por estes dias, várias recomendações para uma navegação segura na internet. À rádio Observador, Bruno Castro, presidente executivo da empresa de cibersegurança Visionware, explica que o tema do novo **coronavírus "acaba por ser um novo isco para fraudes de cibernautas"**. Contudo, as medidas que devemos tomar são as mesmas que temos de ter noutras alturas de grande afluência na internet, como a Black Friday.

> "Trabalhar remotamente não é trabalhar [fisicamente] numa organização, em que estou protegido por ela", explica Bruno Castro.

Como conta o especialista em cibersegurança, por estes dias, "há mais informação a circular". "A nossa sociedade já vivia baseada na internet, isto veio de alguma forma concretizar o que já sabíamos", continua. Como explica a Polícia Judiciária (PJ) em comunicado, **"os contextos de crise de proporções internacionais são,**

tradicionalmente, explorados por atores hostis do ciberespaço para sustentarem as suas campanhas de ciberataques no alarmismo social e na atenção mediática global sobre o tema".

> A atual pandemia associada à propagação do vírus COVID-19 não tem sido exceção, tendo este tema sido selecionado por um número elevado de agentes de ciberameaças como cobertura para as suas campanhas de ciberataques", avança a PJ.

Mas quais são as principais ameaças, principalmente nesta altura?

Como explica a PJ, as principais ameaças são:

- "**As campanhas de *phishing* (por email, SMS ou por redes sociais)** a coberto da imagem de entidades oficiais como a Organização Mundial de Saúde, a UNICEF ou centros de investigação e laboratórios do setor da saúde, com conteúdos alusivos à pandemia, inclusive ficheiros em anexo, e orientado para a captação de dados pessoais das vítimas ou para a infeção dos seus dispositivos com malware;
- A **divulgação de plataformas digitais ou de aplicações [apps] para dispositivos móveis que aparentam divulgar informação em tempo real sobre a pandemia** (exemplo de mapas dinâmicos de contágio, mas que estão, na realidade, orientados para a infeção de equipamentos com *malware* [programas informáticos com objetivo de roubar dados], inclusive da tipologia do *ransomware* [táticas de exortação monetária online];

No aviso acima convém relembrar que, nesta quarta-feira, o Centro Nacional de Cibersegurança alertou para não confiar nem instalar a aplicação COVID-19 Tracker no telemóvel. Trata-se de um destes esquemas de *ransomware* para equipamentos com sistema operativo Android, que, após a sua instalação, "bloqueia o dispositivo e exige um resgate" em bitcoins (moedas digitais). Informações sobre a Covid-19 devem ser recolhida nos sites da Direção-Geral da Saúde e da Organização Mundial de Saúde.

- **Esquemas de fraude digital partilhados por email ou em redes sociais, que divulgam iniciativas de *crowdsourcing*** [campanhas digitais para angariar fundos] para a recolha de donativos para falsas campanhas de compra de material médico ou de proteção pessoal.
- **SMS enviados informando que, de acordo com a lei, estão a ser aplicadas medidas extraordinárias para o combate ao COVID-19, e que todos os cidadãos nacionais serão vacinados**, sendo garantido um reembolso dos custos pelo governo. Para tal, bastaria pagar uma determinada quantia indicada no SMS e através do registo no *link* enviado seriam posteriormente ressarcidos."

Isto significa que devo afastar-me do computador ou do smartphone? Não me digam isso

Claro que não. Há riscos em maior volume nesta fase. Contudo, são — na sua forma — aqueles que já existiam no passado, em momentos de grande tráfego na internet. Por isso, os cuidados que temos de ter agora são muito semelhantes aos que já tínhamos noutras alturas, como já explicavamos em novembro, durante a Black Friday. Os cuidados a ter são os que já foram apresentados por empresas como a Check Point Software e a Kaspersky:

- Principalmente para quem está em teletrabalho, **é importante fazer cópias de segurança regulares dos dados**, de forma a evitar que os ficheiros pessoais se percam em caso de ciberataque;
- **Manter as aplicações atualizadas —** há também muitos programadores a trabalhar remotamente para garantir que continuamos a navegar seguros;
- Não **clicar em hiperligações que sejam recebidas via e-mail ou redes sociais** de endereços desconhecidos.

> Nada disto é novo. O que está a acontecer é o *pishing*, que também recebemos no Black Friday, por exemplo, com tentativas para roubar a passe, números de cartão de crédito, etc", explica Bruno Castro.

Ter **o software antivírus atualizado e ativado** (várias empresas, como a Avast, disponibilizam opções gratuitas online)

No caso de estar a fazer compras online as recomendações são:

- **Navegar apenas em sites seguros** (que tenham "https", com o "s", antes do endereço);
- **Rever a política de devolução** (para não ter surpresas e garantir os seus direitos como consumidor, mesmo num Estado de Emergência há direitos);
- **Desconfiar de todas as ofertas nas redes sociais** (não há almoços grátis no consumo, confirme três vezes antes de aceitar).
- **Utilizar apenas métodos de pagamento seguros** (com o MbNet, pelo MbWay, ou o Paypal, por exemplo).

No caso do teletrabalho, a organização na qual trabalha — caso ainda não o tenha feito — deverá disponibilizar ferramentas para estar protegido quando estiver ligado à rede da empresa. Como explica Elsa Veloso, presidente executiva da DPO Consulting, advogada e especialista em privacidade de dados e segurança da informação, as empresas devem "selecionar e restringir os direitos de acesso em redes internas (como a utilização de VPN)" e alertar os colaboradores para boas práticas.

Por fim, nesta fase, tem também de ter um papel próativo na utilização da internet. Ou seja, se recebeu uma mensagem de WhatsApp de fonte incerta ou leu um artigo de um site não confiável, partilhar é a pior solução. Muitas vezes, os piratas informáticos utilizam estas táticas para aceder a dados de localização, definir padrões de utilização dos utilizadores ou, apenas, espalhar notícias falsas para criar destabilização.