INTERNET SEGURA

#LerAntesClicarDepois

REPÚBLICA PORTUGUESA
SECRETÁRIO DE ESTADO DA DIGITALIZAÇÃO E DA MODERNIZAÇÃO ADMINISTRATIVA

CNCS Centro Nacional de Cibersegurança PORTUGAL

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

PREFÁCIO

As tecnologias digitais são cada vez mais uma parte integrante da nossa vida e daquilo que fazemos todos os dias. Seja na forma como trabalhamos, como compramos ou como nos relacionamos com outras pessoas, seja até de muitas outras maneiras que talvez nem imaginemos, o digital está presente para facilitar a nossa vida, levando-nos onde a distância, o tempo e as complicações antes nos impediam de chegar.

Somos utilizadores e utentes do digital. Devemos ser, cada vez mais, cidadãs e cidadãos digitais. Isso significa usar o digital de forma exigente, crítica e consciente. Consciente dos riscos que, de forma mais ou menos evidente, ocorrem no ciberespaço, no mundo das redes e sistemas informáticos em que a vida digital circula. Mas conscientes, também, da nossa responsabilidade, enquanto membros de uma comunidade, em contribuir para um ciberespaço seguro para todas as pessoas.

Nesta dimensão onde tudo é fácil, rápido e acessível, é importante, por isso, conhecer e identificar os riscos - para prevenir e reagir de forma adequada. Se a nossa vida é cada vez mais digital, é natural que apliquemos no ciberespaço a mesma dose de cuidado que usamos no mundo físico. Se aqui usamos cinto de segurança ou capacete, se trancamos a porta de casa ao sairmos ou se paramos ao sinal vermelho, quais são os equivalentes destes cuidados no ciberespaço e porque é que os devemos ter? É isso que convido a conhecer. Mas na dúvida, já sabe: para usar a Internet com segurança, leia antes e clique depois.

Mário Campolargo

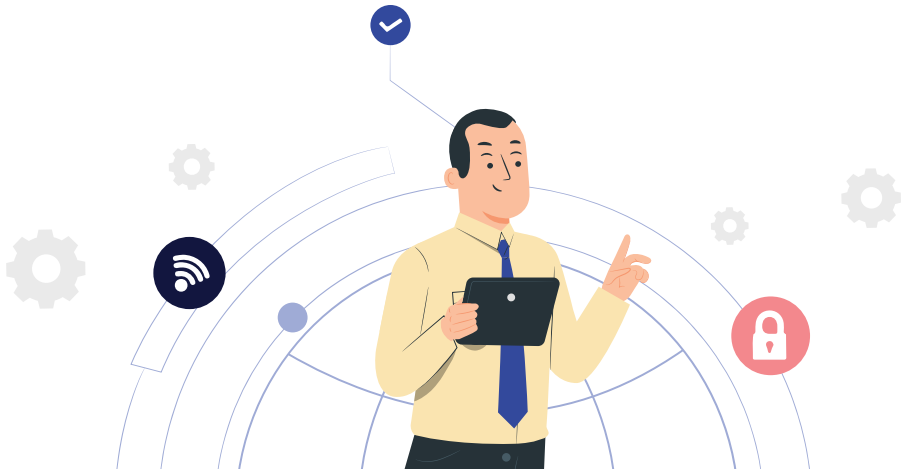
Secretário de Estado da Digitalização e da Modernização Administrativa

A CIBERSEGURANÇA É PARA SI

A cibersegurança não é apenas um assunto de profissionais de informática. É uma responsabilidade de todas as pessoas que utilizam tecnologias digitais e de quem toma decisões que afetam a vida das organizações. Por isso, é importante que cada cidadã ou cidadão, no uso corrente do digital ou na responsabilidade que assume, tenha conhecimento das boas práticas diárias no ciberespaço (a sua ciber-higiene).

O QUE É EXATAMENTE A CIBERSEGURANÇA?

A cibersegurança refere-se a todas as práticas que procuram garantir um uso seguro do ciberespaço – ou seja, o espaço comum de quem utiliza as redes e os sistemas informáticos, como sejam os dispositivos móveis onde acedemos à Internet e às redes sociais ou os computadores que usamos nas nossas profissões. A cibersegurança está presente desde a prevenção até à reação a incidentes de segurança informática, incluindo não só a tecnologia, mas também os comportamentos necessários a usá-la de forma adequada. Muitos dos incidentes resultam do desconhecimento sobre os melhores cuidados a ter, mas também da exploração de fragilidades dos utilizadores por parte de cibercriminosos.



ANALISAR AS INSTRUÇÕES DE EMAILS, SMS, MENSAGENS INSTANTÂNEAS OU TELEFONEMAS SUSPEITOS

Sempre que receber uma mensagem por *email*, SMS, numa rede social, ou um telefonema a solicitar informações sensíveis e dados pessoais, ou pedindo que clique num *link* ou num anexo, em nome de uma organização considerada credível (um Banco ou um serviço postal, por exemplo) deve tentar perceber se faz sentido esse pedido e se é mesmo efetuado pela entidade representada. Quando receber contactos deste tipo, é muito importante não partilhar dados sensíveis ou clicar em *links* e anexos.

Porquê? Uma das técnicas utilizadas pelo cibercrime é o envio de *emails*, SMS, mensagens instantâneas ou telefonemas para potenciais vítimas para que estas revelem informações sensíveis ou instalem programas maliciosos nos seus dispositivos. Para o efeito, os cibercriminosos simulam uma marca fidedigna de modo a ludibriar o destinatário. É o chamado *phishing*, quando se procura recolher esta informação através de *email*, ou *smishing*, quando realizada por SMS ou mensagem instantânea. Por vezes também ocorre através de telefonema, e aí intitula-se *vishing*.

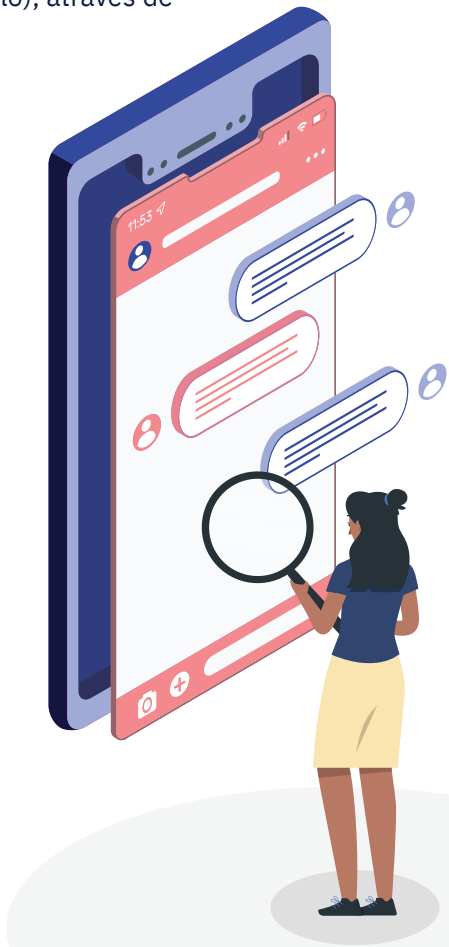
Sabia que? O *phishing* e o *smishing* são os tipos de incidentes mais registados pela equipa de resposta a incidentes de cibersegurança do CNCS (CERT.PT).

CONFIRMAR INFORMAÇÃO SENSÍVEL QUE É PEDIDA POR EMAIL, SMS, MENSAGENS INSTANTÂNEAS OU TELEFONEMAS

Uma das formas de combater as burlas através de *emails*, SMS, mensagens instantâneas e telefonemas é verificar junto de outras fontes a veracidade dos pedidos realizados através destes meios. Por exemplo, se alguém solicita uma transferência bancária, é muito importante confirmar esse pedido junto de uma terceira pessoa (o destinatário ou uma chefia, por exemplo), através de outro meio de contacto.

Porquê? Os cibercriminosos utilizam como uma das suas técnicas a simulação de um pedido de uma transferência bancária por parte de uma chefia ou de um fornecedor a um empregado de uma organização, mas que acabará por ser feita para uma conta não legítima. Outra técnica utilizada é a de conduzir, por telefone, os vendedores de produtos em plataformas *online* a realizarem pagamentos em lugar de recebimentos relativamente a um suposto comprador. Alguns cibercriminosos simulam ainda ser um parente de uma potencial vítima pedindo-lhe dinheiro com uma falsa urgência através de mensagens instantâneas.

Sabia que? Têm aumentado de forma significativa os casos da burla correntemente intitulada de "Olá mãe, Olá pai", em que um atacante simula ser o filho de uma potencial vítima, através de uma mensagem instantânea, pedindo-lhe dinheiro com urgência.



DIVERSIFICAR AS PALAVRAS-PASSE

É importante usar palavras-passe fortes (pelo menos 12 caracteres de tipo diversificado, sem palavras associadas ao utilizador), ter uma diferente por cada plataforma que se usa, alterar as que são atribuídas pelo fabricante ou instalador (no Wi-Fi doméstico, por exemplo) e não as partilhar com ninguém.

Porquê? Muitos dos acessos ilegítimos a contas *online* ocorrem porque alguém conseguiu descobrir a palavra-passe. Por isso, é importante ter palavras-passe suficientemente fortes para resistirem a programas que as identificam por tentativa-erro ou a descobertas por adivinhação.

Sabia que? Muitos ciberataques que colocaram em causa grandes organizações começaram através da intrusão de um cibercriminoso numa conta *online* de um empregado.

USAR MÚLTIPLO FATOR DE AUTENTICAÇÃO

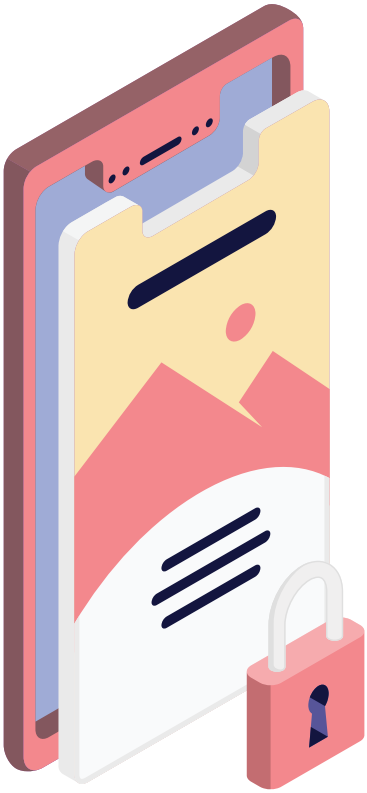
O múltiplo fator de autenticação é uma forma de garantir que a segurança das contas *online* não fica exclusivamente dependente da palavra-passe. Através deste mecanismo, sempre que alguém procura aceder a uma conta, tem de acionar pelo menos um segundo fator de autenticação para entrar na conta, para além da palavra-passe– por exemplo, a introdução de um código enviado por SMS para o telemóvel do utilizador. Por esta razão, sempre que possível, deve ativar-se esta funcionalidade.

Porquê? Ter o múltiplo fator de autenticação ativado evita que uma palavra-passe que possa ter sido descoberta por um cibercriminoso através, por exemplo, do furto de listas com dados pessoais, seja utilizada para aceder à informação, prevenindo a intrusão.

Sabia que? Muitos ciberataques resultam na divulgação de dados pessoais de clientes de organizações, entre os quais palavras-passe que depois são usadas por cibercriminosos para realizar intrusões.

REALIZAR CÓPIAS DE SEGURANÇA E ATUALIZAÇÕES REGULARES

É fundamental realizar cópias de segurança regulares dos dados considerados mais importantes, para dispositivos de armazenamento não ligados à Internet. Além disso, os utilizadores de qualquer tecnologia digital devem manter os sistemas e as aplicações atualizados, seja num computador pessoal, num portátil ou num telemóvel.



Porquê? Existem ataques que bloqueiam o acesso a informação relevante dos sistemas e aplicações atacados (cifrando bases de dados, por exemplo), de modo que essa informação apenas possa ser libertada mediante o pagamento de uma quantia a quem faz o ataque. Esta forma de extorsão é o chamado ataque de "*ransomware*". Manter uma cópia de segurança da informação sempre atualizada permite recuperá-la na eventualidade de ataque, sem necessidade de pagar o "resgate". Note-se ainda que os fornecedores de sistemas e aplicações digitais atualizam os seus produtos regularmente com correções de segurança que permitem eliminar vulnerabilidades técnicas, pelo que é fundamental promover a atualização regular de dispositivos e de *software*.

Sabia que? O *ransomware* é uma das ameaças que tem aumentado mais e causa muitos impactos nas organizações.

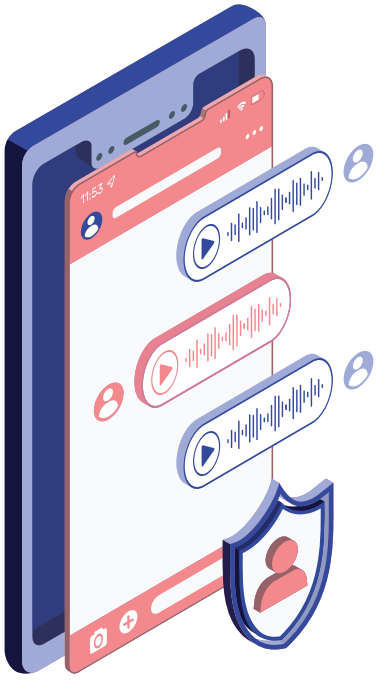
Todos os anos são descobertas novas vulnerabilidades em sistemas e em aplicações de uso generalizado, que são aproveitadas como pontos de entrada de ciberataques em todo o mundo.

EVITAR PARTILHAR INFORMAÇÃO SENSÍVEL E NOTÍCIAS QUE PODEM CONTER DESINFORMAÇÃO NAS REDES SOCIAIS

A informação que partilhamos nas redes sociais pode muitas vezes ser sensível e comprometer a nossa privacidade e a de outras pessoas. Por isso, é importante ponderar os riscos que possam decorrer da partilha dessa informação, antecipando o uso que dela pode ser feito. Devemos também ter atenção às opções de privacidade das várias plataformas na Internet, escolhendo as que sejam mais adequadas às expetativas que temos ao usá-las. Além disso, é importante avaliar a veracidade de certos conteúdos antes de os partilhar, de modo a evitar a proliferação de desinformação destinada a atingir objetivos muitas vezes obscuros. Isto passa por verificar se a fonte da informação que se partilha é um meio de comunicação social credível ou por procurar outras fontes que confirmem a informação.

Porquê? A divulgação da vida privada nas redes sociais pode expor os utilizadores, inconscientemente, a várias formas de abuso. Os cibercriminosos utilizam as redes sociais para recolher informações sobre potenciais vítimas que possam ser alvos de ataques, como sejam burlas ou *phishing*. Além disso, a lógica de partilha de conteúdos pelos utilizadores inerente ao modelo de funcionamento das redes sociais pode favorecer a disseminação de desinformação. O utilizador é um veículo de divulgação de notícias falsas.

Sabia que? Portugal é um dos países da União Europeia com mais utilizadores de redes sociais. A seguir à televisão, as redes sociais são a fonte de notícias mais frequente no país.



NÃO USAR PEN USB DE ORIGEM DESCONHECIDA OU WI-FI PÚBLICA SEM VPN

A forma como os utilizadores conectam dispositivos e redes Wi-Fi tem implicações na sua segurança. Dispositivos como as pen USB devem ser utilizados com cautela, conhecendo a sua proveniência. No caso das redes de Wi-Fi públicas, a ligação de dispositivos a estas deve ser feita preferencialmente através de uma rede virtual privada (VPN), que evita que a navegação *online* seja monitorizada por estranhos. Quando há desconhecimento sobre a origem de uma pen USB ou sobre a gestão de uma rede Wi-Fi, os cuidados devem ser redobrados.

Porquê? Uma pen USB de origem desconhecida ou suspeita pode ser um veículo para a disseminação de programas maliciosos. É importante usar pen USB de confiança, de preferência adquiridas pelo próprio utilizador. As redes públicas Wi-Fi, por sua vez, podem ser comprometidas por quem, com alguns conhecimentos técnicos, tenha a intenção maliciosa de monitorizar as atividades de outros utilizadores também ligados.

Sabia que? Existem casos famosos de incidentes de cibersegurança com elevado impacto que se julga terem sido iniciados com o uso de uma pen USB de origem desconhecida, a qual estaria comprometida com um programa malicioso.

FAZER COMPRAS ONLINE COM CUIDADO

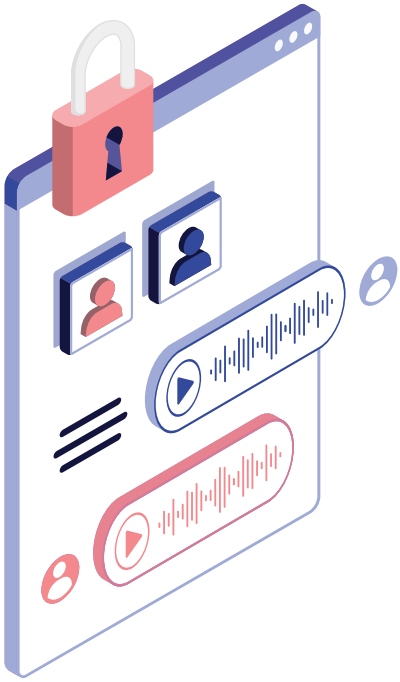
As compras *online* devem ser realizadas com o cuidado de evitar burlas e o furto de informação sensível, como números de cartões de crédito. É importante recolher informação sobre o vendedor para garantir que é fidedigno e desconfiar de ofertas boas demais para serem verdade. Formas de pagamento mais seguras, como os cartões de crédito temporários ou as carteiras digitais, devem ser consideradas neste tipo de compras.

Porquê? Várias burlas são feitas através da venda fraudulenta de produtos e serviços *online*, muitas vezes porque os produtos e serviços não existem efetivamente ou não correspondem ao anunciado. Alguns *sites* fraudulentos podem recolher dados sobre os números de cartões de crédito dos utilizadores para uso malicioso.

Sabia que? As burlas *online* são os crimes praticados em contexto digital mais participados às autoridades em Portugal.

PREVENIR E COMBATER O CYBERBULLYING E A EXTORSÃO SEXUAL

O ciberespaço é também um espaço de relacionamentos entre pessoas, nomeadamente através das redes sociais. Por isso, é importante ter alguns cuidados para evitar abusos. Para resistir ao *bullying online* (ou *cyberbullying*), é importante evitar retaliações a qualquer tipo de agressão, não responder a mensagens intimidatórias e bloquear quem aparece sistematicamente como agressor. Um outro tipo de caso neste contexto é a extorsão sexual por meios digitais, isto é, extorsão com base na ameaça de divulgação de conteúdos íntimos de teor sexual de uma vítima. Nestes casos, não se deve pagar qualquer valor ou partilhar conteúdos. Em ambas as situações, é importante registar as interações realizadas com o agressor e denunciar o caso às autoridades.



Porquê? Existem utilizadores do ciberespaço que se aproveitam das capacidades de anonimização e de disseminação de conteúdos proporcionadas pela esfera digital para abusarem de relacionamentos ou de interações sociais *online*.

Sabia que? O *cyberbullying* e a extorsão sexual são das formas de violência *online* mais denunciadas à APAV todos os anos.

LINHAS DE APOIO

Contacte a Linha Internet Segura, para o número

800 219 090

ou o *email*

linhainternetsegura@apav.pt

Para reportar um incidente ou um cibercrime, utilize os seguintes contactos:

CERT.PT (CNCS) **cert@cert.pt**

Polícia Judiciária **unc3t@pj.pt**

Procuradoria-Geral da República **cibercrime@pgr.pt**

INTERNET SEGURA
#LerAntesClicarDepois