Boas práticas no uso de smartphones

Neste Documento

› A. Objetivo
› B. Como
› C. O que corre bem quando age bem
› D. Porquê o cuidado
› E. Sabia que?
› F. Dados

OBJETIVO: GARANTIR UMA UTILIZAÇÃO MAIS SEGURA DOS *SMARTPHONES*

Como?

a. Ative os mecanismos de bloqueio do seu *smartphone* através de um PIN ou de outra funcionalidade de autenticação;
b. Utilize uma VPN sempre que se ligar a uma Wi-Fi pública ou então opte por utilizar os dados para aceder à Internet em lugares sem Wi-Fi doméstico ou profissional;
c. Evite ter o *bluetooth* e a localização do seu *smartphone* ligados desnecessariamente;
d. Mantenha o sistema e as aplicações atualizados;
e. Seja cuidadoso com as aplicações que instala: opte pelas que são disponibilizadas por plataformas reconhecidas; verifique se as revisões de utilizadores e especialistas são positivas; limite o acesso das aplicações apenas às funcionalidades essenciais ao seu funcionamento;
f. Opte pelas configurações de segurança e privacidade do seu *smartphone* e aplicações mais restritas;
g. Não clique em *links* enviados através de SMS suspeitos;
h. Não atenda chamadas de números identificados como fraude ou sobre os quais tenha suspeitas;
i. Sempre que alguém lhe telefonar em nome de um serviço pedindo dados pessoais, ou solicitando que faça uma transferência bancária, ou ainda sugerindo que instale algo no seu dispositivo informático, certifique-se de que está a falar com alguém fidedigno, confirmando o pedido noutras fontes e questionando a veracidade do que lhe é solicitado.

O que corre bem quando age bem

- Protege os seus dados pessoais e profissionais e a multiplicidade de acessos a plataformas que o seu *smartphone* permite.

Porquê o cuidado

O *smartphone* tornou-se num objeto nuclear para o uso do ciberespaço, na medida em que é um dispositivo que não é apenas um telemóvel, mas um autêntico computador de bolso onde se encontram múltiplas funcionalidades. Esta importância nem sempre é acompanhada pela correspondente

Sendo um objeto móvel, o *smartphone* acompanha de muito perto a vida de cada indivíduo, guardando vestígios do quotidiano como poucos dispositivos: as imagens partilhadas; as deslocações feitas com ajuda do GPS; a corrida acompanhada por uma aplicação; o histórico de mensagens e telefonemas; entre muitos outros aspetos. Quando o *email* profissional ou outras aplicações usadas para interações profissionais estão disponíveis no *smartphone,* também os dados do contexto de trabalho ficam em risco no caso de não se terem todos os cuidados. Quando se protege o *smartphone,* protege-se o acesso a toda esta informação.

Sabia que?

O comprometimento de um *smartphone* através de furto ou de um simples extravio pode colocar em causa muita informação que interessa proteger, sobretudo se não tiver ativado nenhum mecanismo de boqueio do dispositivo. Acresce que um programa malicioso instalado no *smartphone* que permita espiar a atividade do utilizador através da câmara de filmar, por exemplo, pode ter consequências extremamente invasivas da privacidade. Além disso, muitas vezes o *smartphone* é utilizado como segundo fator de autenticação através de um SMS, de um *token* ou de um *email.* Por isso, o comprometimento deste dispositivo pode ajudar um agente malicioso a contornar a camada extra de segurança que o múltiplo fator de autenticação permite.

Muitas das fraudes realizadas através da chamada "engenharia social" são feitas utilizando telefonemas para capturar dados pessoais ou conduzir as pessoas a fazer transferências bancárias. A essas chamadas telefónicas chama-se *vishing,* palavra que resulta da contração da palavra "voz" com a palavra *"phishing".* Portanto, trata-se de um *phishing* através de voz em vez de *email.* Esta técnica também é muito utilizada através de SMS, o chamado *smishing* (contração de "SMS" com *"phishing"),* onde frequentemente é partilhado um *link* que pode conduzir a *websites* fraudulentos ou à instalação de *software* malicioso.

Também é muito importante manter o sistema e as aplicações atualizadas. Tal como em relação a qualquer computador, estas atualizações permitem corrigir vulnerabilidades de segurança que vão sendo descobertas ao longo do tempo. Também como num computador, o acesso a Wi-Fi públicas deve ser feito através de uma VPN, evitando-se assim as vulnerabilidades de segurança que se encontram numa rede pública, as quais podem permitir o acesso de um estranho com os conhecimentos adequados. Em alternativa, nesses casos, é preferível utilizar os dados da operadora.

Considerando que o *smartphone* é um dispositivo onde facilmente se instalam novas aplicações, muitas delas "aparentemente" gratuitas, é preciso ter algum cuidado com os critérios que são utilizados para fazer estas instalações e com as autorizações de acesso a funcionalidades que são atribuídas. As aplicações disponibilizadas fora das plataformas reconhecidas para o efeito são menos sujeitas a verificação e crítica. É mais provável encontrar uma aplicação maliciosa nesse contexto, a qual pode trazer consigo *software* que, por exemplo, espie os utilizadores e viole os seus dados pessoais *(spyware).* Além disso, mesmo aplicações que não instalam *software* malicioso podem ser abusivas relativamente aos utilizadores, acedendo sem necessidade à câmara de filmar, a fotografias ou à lista de contactos, existindo a possibilidade desses dados serem usados para fins comerciais não autorizados. Uma aplicação pela qual não se paga através de dinheiro é geralmente uma aplicação que se paga através dos dados do utilizador.

Dados

- Em 2020, existem cerca de 13 milhões e meio de assinaturas de serviços móveis em Portugal (Portada, 2021);
- Apenas 42% dos indivíduos em Portugal, em 2020, afirmam alguma vez ter recusado ou restringido o acesso a dados pessoais, quando usaram ou instalaram uma aplicação no *smartphone* – a média da UE é de 52% (Eurostat, 2020);
- Apenas 11% dos indivíduos em Portugal, em 2020, reconhecem ter instalado ou subscrito algum sistema de segurança no seu *smartphone* – o mesmo valor do que a média da UE (Eurostat, 2020);
- O *phishing* e o *smishing* são o tipo de incidentes mais registados pelo CERT.PT em 2020, correspondendo a cerca de 43% dos incidentes durante esse ano (CNCS, 2021).

Última atualização em 05-04-2022

AVISOS LEGAIS

GLOSSÁRIO

CERT.PT

Morada:
Rua da Junqueira 69,
1300-342 Lisboa

Telefone:
(+351) 210 497 399

Email:
cert@cert.pt

CNCS

Morada:
Rua da Junqueira 69,
1300-342 Lisboa

Telefone:
(+351) 210 497 400

Email:
cncs@cncs.gov.pt

Horário:
Seg - Sex
9h00 às 17h00

SAIBA MAIS

Quero subscrever a newsletter e eventos do CNCS no meu email.

SEJA O PRIMEIRO A SABER:

Endereço de Email ENVIAR

Noticias

Eventos

Alertas

GNS REPÚBLICA PORTUGUESA PRESIDÊNCIA