Boas práticas nas redes sociais

Neste Documento

OBJETIVO: GARANTIR UMA UTILIZAÇÃO MAIS SEGURA DAS REDES SOCIAIS

Como?

1. Aceite apenas ligações de pessoas conhecidas;
2. Não indique o número de telemóvel ou morada no seu perfil ou em *posts;*
3. Evite partilhar informação que revele locais, imagens de crianças ou dados sensíveis;
4. Confirme a veracidade das notícias que partilha – verifique sempre a fonte;
5. Não clique em posts e *links* suspeitos – alguns podem ser *phishing* ou *software* malicioso;
6. Utilize palavras-passe únicas e complexas para aceder às redes sociais e altere-as com frequência;
7. Opte pelas definições de privacidade mais restritas;
8. Ative o bloqueio automático do *smartphone* e o uso de PIN ou palavra-passe;
9. Não faça *login* a outros serviços através de contas das redes sociais.

O que corre bem quando age bem

• Mantém a sua informação pessoal mais segura;
• Fica mais protegido contra roubo de contas e perfis;
• Protege as crianças de possíveis ameaças;
• Evita a propagação de notícias falsas.

Porquê o cuidado

Porque as redes sociais são um meio que agentes de ameaças usam com o fim de recolher informação sensível sobre possíveis vítimas. Essa informação

A partir do momento que divulga algo numa rede social, alguém pode copiar esse conteúdo e partilhar com outros. As mensagens por WhatsApp também podem ser divulgadas a terceiros e existem casos em que o sistema de cifra é comprometido. Acresce que, ao publicar uma imagem, abdica dos direitos sobre a mesma. Existem redes criminosas que constroem bases de dados com imagens de crianças com objetivos maliciosos. Os pais devem ter o cuidado de não partilhar imagens dos filhos sem a sua autorização *(sharenting),* sempre que possível.

As redes sociais têm uma componente comercial. Quando faz um "gosto" num *post,* ajuda a criar um perfil para publicidade orientada a determinado público-alvo. Quando acede a plataformas utilizando contas de redes sociais, partilha os seus dados com essas plataformas. Deverá ser informado dessa situação, tendo a opção de escolha nesse momento. Os casos de utilização abusiva de dados de redes sociais têm aumentado muito nos últimos anos.

O *phishing* nestas plataformas também tem crescido muito. Esta forma de recolher informação sensível através de manipulação, ou engenharia social, não acontece apenas mediante *email* ou SMS *(smishing).* Através de *posts* é possível conduzir os utilizadores a partilharem informação privada, como números de cartões de crédito. Existem também campanhas de SPAM e *phishing* lançadas através dos sistemas de mensagens das redes sociais.

Igualmente preocupante é o uso que se faz das redes sociais para disseminar desinformação (vulgo Fake News), com objetivos políticos ou económicos. A partilha de notícias falsas encontra nestas redes uma forma de propagação muito importante. Por cada gosto e partilha que um utilizador faz, o conteúdo em causa é promovido. No caso de se tratar de desinformação, ao divulgar este tipo de materiais, o utilizador torna-se conivente e uma peça fundamental para a propagação de informação que não é verdadeira. Acresce que muitos dos perfis e respetivas partilhas são assentes em contas falsas ou na atividade de uma *botnet*.

Por fim, é essencial referir que certos casos de roubo de identidade acontecem através da apropriação de contas de redes sociais, servindo para causar danos reputacionais em terceiros ou trazer benefícios económicos aos agentes maliciosos. Devido ao seu caráter social e interativo, estas plataformas são um dos principais veículos de *cyberbullying.* A exposição que proporcionam permite que *bullies* e *trolls* explorem a informação disponível para perseguirem e agredirem (através de conteúdos) as suas vítimas e que crianças fiquem sujeitas a assédio *online* por parte de adultos *(grooming).*

Dados

• Os ataques dirigidos a indivíduos e organizações específicos através de redes sociais é uma tendência crescente em 2020.

• Outra tendência em 2020, que vem de anos anteriores, é o uso das redes sociais para campanhas de desinformação que procuram manipular os cidadãos com fins políticos. (ENISA Threat Landscape, 2020)

• Em 2019, o condicionamento de partilha de informação pessoal nas redes sociais foi a limitação que os indivíduos em Portugal mais colocaram a si próprios fruto de preocupações de segurança no uso da Internet, em 32,6% dos inquiridos. (IUTIC Famílias, INE, 2019)

• Em Portugal, em 2019, apenas 16% dos indivíduos admitem ter alterado a palavra-passe de uma conta de rede social durante os 12 meses anteriores. A média da UE no mesmo ano é de 25%. (Eurobarómetro especial 499, 2020)

• 37% dos indivíduos em Portugal, em 2020, admitem utilizar contas de redes sociais como procedimento de *login* a outros serviços *online.* A média da UE é de 35%. (Identification procedures used for online services, Eurostat, 2021)

Última atualização em 23-08-2021

SOBRE NÓS

O que é a cibersegurança?
Missão do CNCS
O que fazemos
História do CNCS
Trabalhar no CNCS
Enquadramento legal

AVISOS LEGAIS

GLOSSÁRIO

(+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