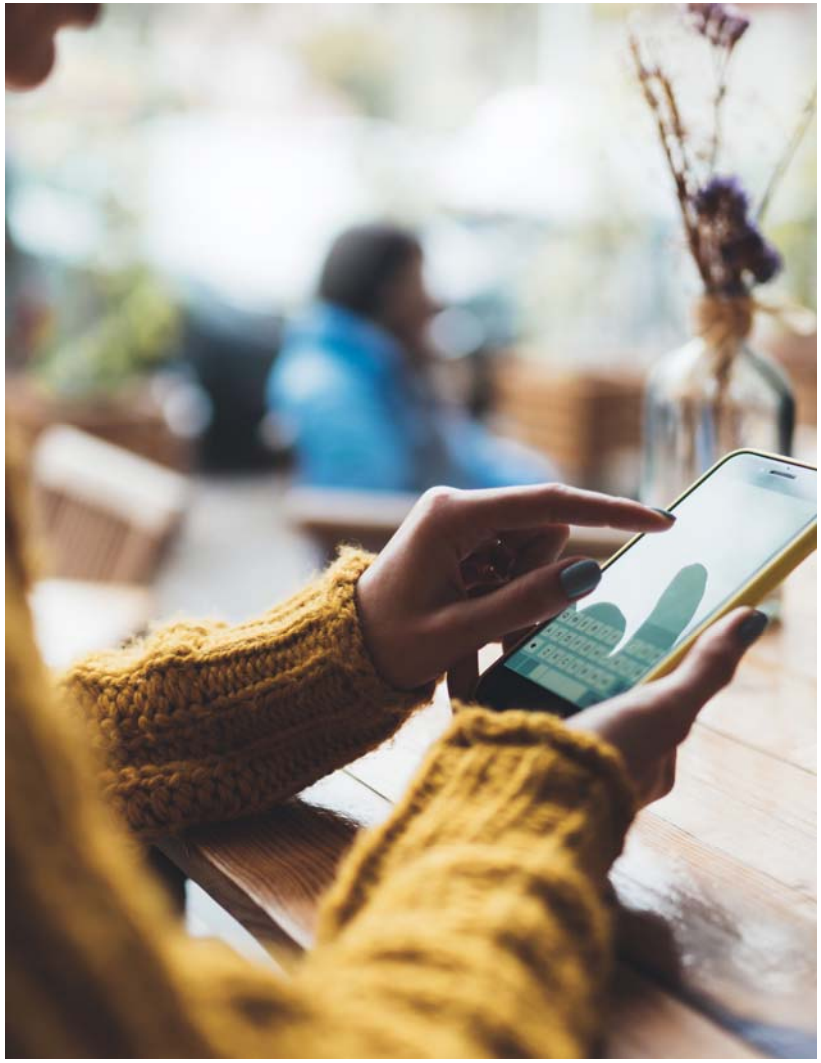
CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

RUTH FERRONY



Índice

A Cibersegurança Hoje..... 3

Análise global..... 6

Fator Humano na Cibersegurança..... 9

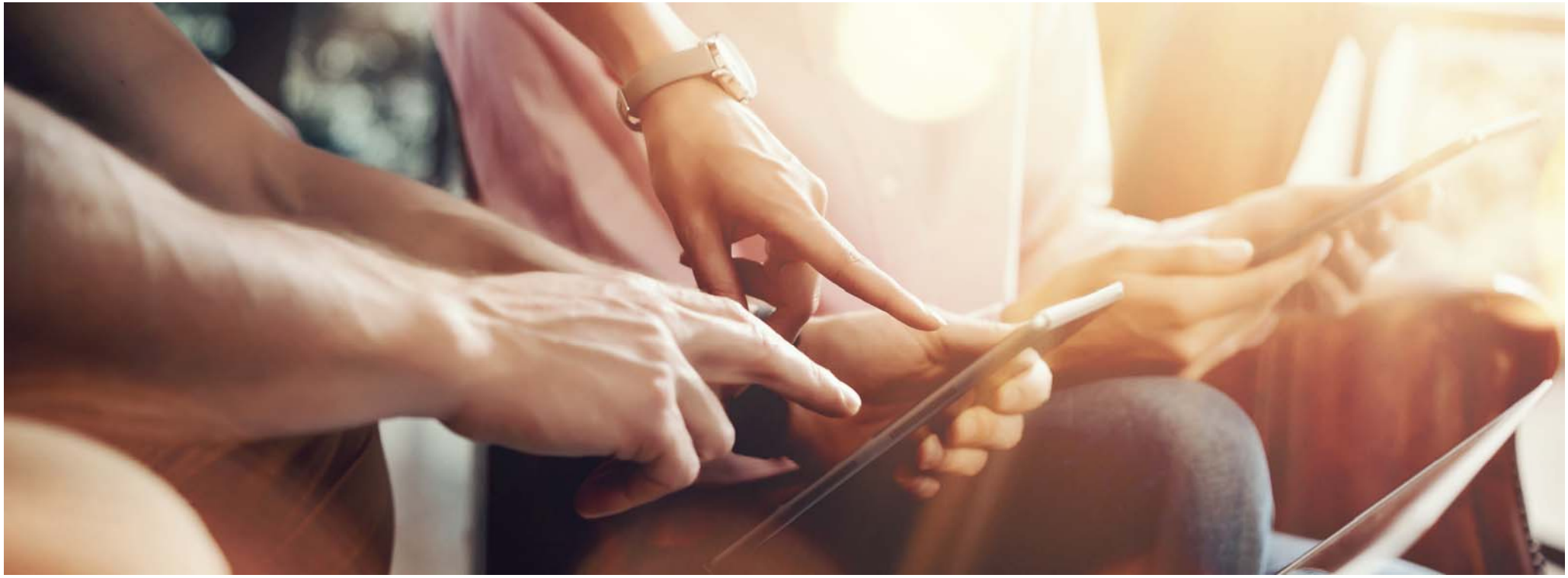
Problema – Solução..... 10

Dispositivos Móveis em ambiente de trabalho... 11

Dispositivos Móveis em ambiente de trabalho... 14

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

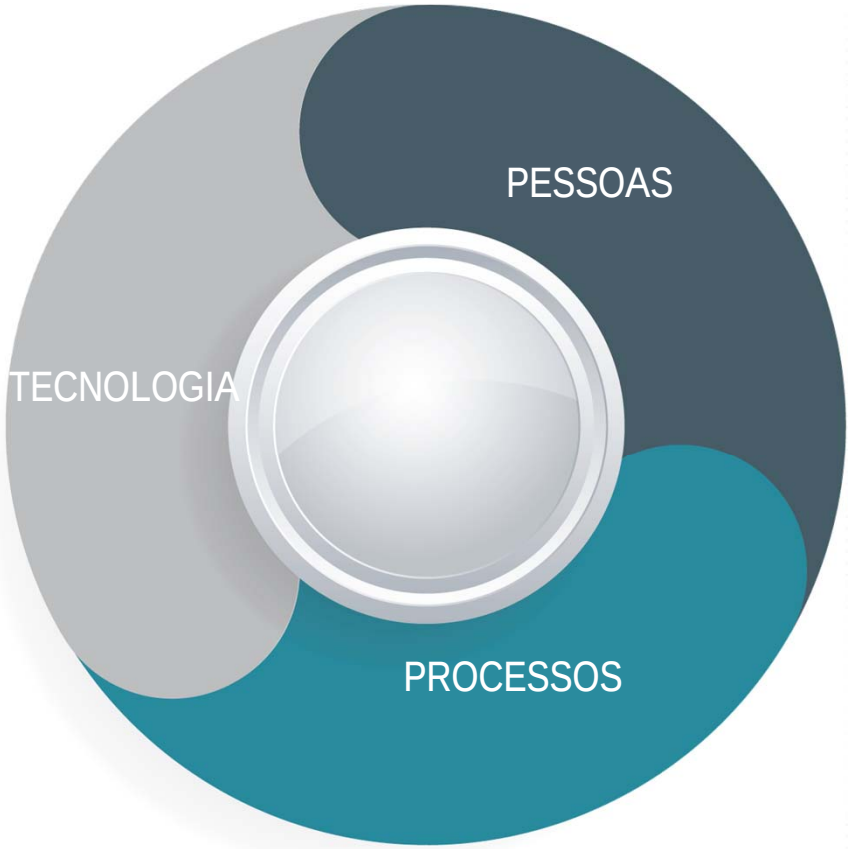
A CIBERSEGURANÇA HOJE



CNCS
Centro Nacional de Cibersegurança PORTUGAL

A **transição digital** exige segurança
O digital como **substituição do presencial** aumenta os riscos
O digital cria **novas ameaças**
Cibersegurança
Um Lugar Central
Os **serviços essenciais** estão mais expostos ao digital
Algumas **ameaças *offline* convertem-se** para o *online*
O digital cria **novas ameaças**

A Cibersegurança é composta por:



ANÁLISE GLOBAL

Os números de incidentes de cibersegurança e de cibercrimes a afetar o ciberespaço de interesse nacional continuaram a aumentar em 2022, verificando-se, em particular, um crescimento significativo de incidentes com elevado potencial disruptivo e de crimes tipificados na Lei do Cibercrime (crimes informáticos).

As ciberameaças a afetar o ciberespaço de interesse nacional em 2022 de modo mais relevante foram o *ransomware*, a cibersa-botagem/indisponibilidade, o *phishing*/*smishing*/*vishing*, a burla *online*, outras formas de engenharia social e o comprometimento de contas/tentativa de *login*.

Em termos de casos com elevado impacto em Portugal, durante o primeiro trimes-tre de 2022 ocorreu um conjunto de ações maliciosas com efeitos muito disruptivos. O ano foi marcado por ataques de *ransomware*, redundando, por vezes, em divulgação de dados.

(CNCS, 2023a)

O ***Phishing*** é um forte vetor de ataque.

O ***Ransomware*** afeta todo o tipo de organização.

O Cibercrime é muito **profissional.**

O contexto **geopolítico e pandémico.**

Os ciberataques são cada vez mais **automatizados.**

As tecnologias emergentes (IoT, 5G, IA, Cloud, HPC, Computação Quântica, ..) colocam novos desafios.

Os **novos modelos de trabalho** são uma realidade.

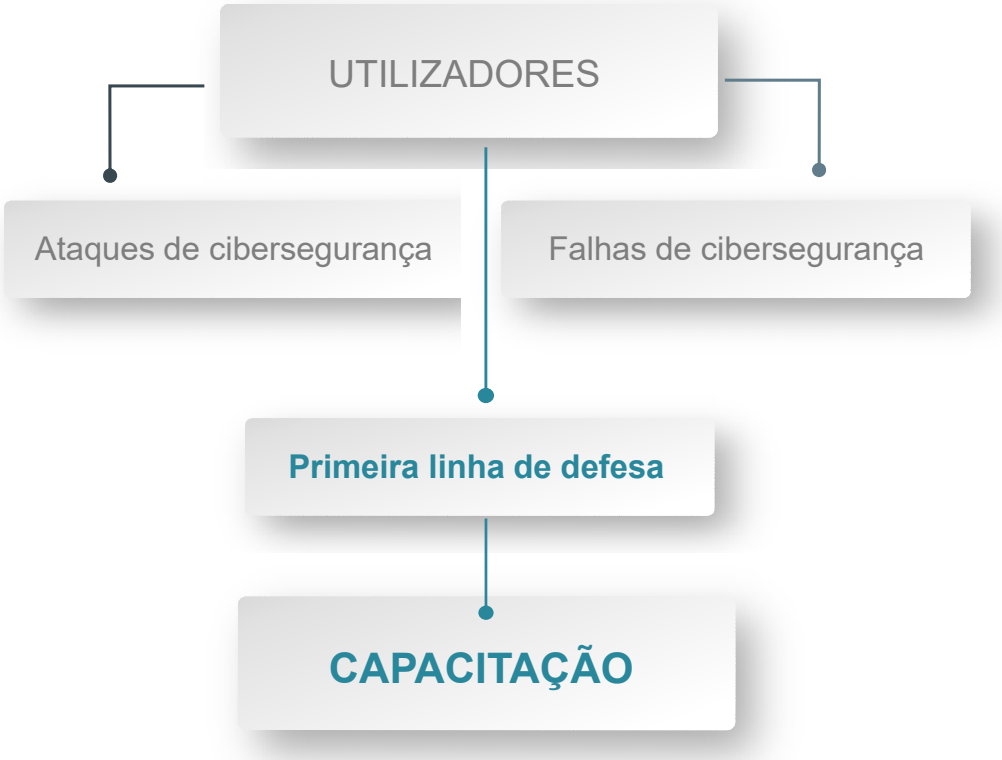
O fator humano continua por **sensibilizar e capacitar.**

O FATOR HUMANO NA CIBERSEGURANÇA

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

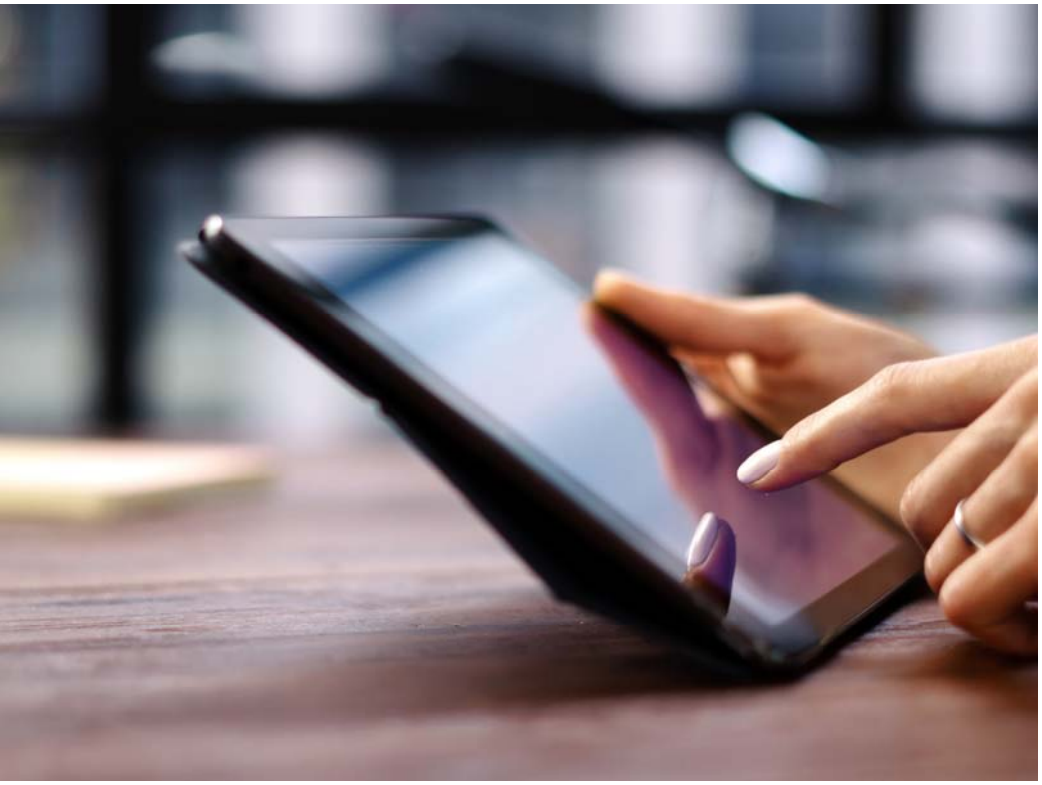
PROBLEMA - SOLUÇÃO

Comportamentos de Risco



Dispositivos Móveis em ambiente de trabalho

CNCS
Centro Nacional de Cibersegurança PORTUGAL



- **Vida profissional versus profissional**
- **Gestão do tempo pessoal – trabalho**
- **Smartphone ao "alcance de 1 dedo":**

  Benefícios versus Problemas - organizações

Smartphone:
Dispositivo que não é apenas um telemóvel!

- Ative os mecanismos de bloqueio do seu *smartphone* através de um PIN ou de outra funcionalidade de autenticação;
- 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;
- Evite ter o *bluetooth* e a localização do seu *smartphone* ligados desnecessariamente;
- Mantenha o sistema e as aplicações atualizados;
- 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;
- Opte pelas configurações de segurança e privacidade do seu *smartphone* e aplicações mais restritas;
- Não clique em *links* enviados através de SMS suspeitos;
- Não atenda chamadas de números identificados como fraude ou sobre os quais tenha suspeitas;
- 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.

Redes Sociais em ambiente de trabalho

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Cyberloafing

É um termo para descrever os trabalhadores que utilizam o tempo de trabalho para participar em actividades não relacionadas com o trabalho na Internet, como a navegação na Web, a utilização de redes sociais ou a verificação e resposta a correio eletrónico pessoal

Vantagens

- Pesquisa
- Descansar a mente
- Saber notícias de familiares/amigos

Desvantagens

- Imersão – tempo excessivo de uso
- Distração
- Tratar de assuntos pessoais

Dicas "etiqueta" no uso das Redes Sociais pessoais
(sobre organização)

- Evitar abordar assuntos de carater sigiloso da organização
- Não criticar ou falar mal da organização e colegas de trabalho – compromete a imagem da organização
- Publicações pessoais em horário de trabalho
- Alerta com fotos do espaço/secretária de trabalho -pode conter informação sigilosa
- Cuidado no tipo de publicações, exposição de fotos

Regra do bom senso, cautela e respeito a todos os níveis – Nunca esquecer a pegada digital! – fornecer demasiada informação.

Cuidados e Boas Práticas

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Cuidar dos Dispositivos

- Utilizar de preferência **dispositivos autorizados** pela organização
- Ser **o único a utilizá-los** – evitar que terceiros os utilizem
- Usar apenas ***pens* USB confiáveis**
- Ativar o **bloqueio** automático dos dispositivos e usar **PIN** ou **palavra-passe**
- Utilizar **filtro** no ecrã do portátil

Cuidar dos Sistemas e dos Dados

- Garantir junto da organização que os dispositivos estão **atualizados** e têm antivírus ativado
- Fazer ***backups*** regulares para um dispositivo externo
- Utilizar **palavras-passe complexas** (com mais de 12 caracteres e não previsíveis), usar **uma por conta, ter Gestor de palavras-passe** e ativar **MFA**

Cuidar da Navegação

- Evitar Wi-Fi de espaços públicos e utilizar **VPN** da organização
- Navegar em *websites* **HTTPS**
- Alterar a **palavra-passe do Wi-Fi doméstico** e garantir que é forte
- Alterar o **nome do Wi-Fi doméstico** para não ser identificado
- Escolher a forma de **cifra** mais forte do Wi-Fi doméstico – WPA2

Cuidar da Comunicação

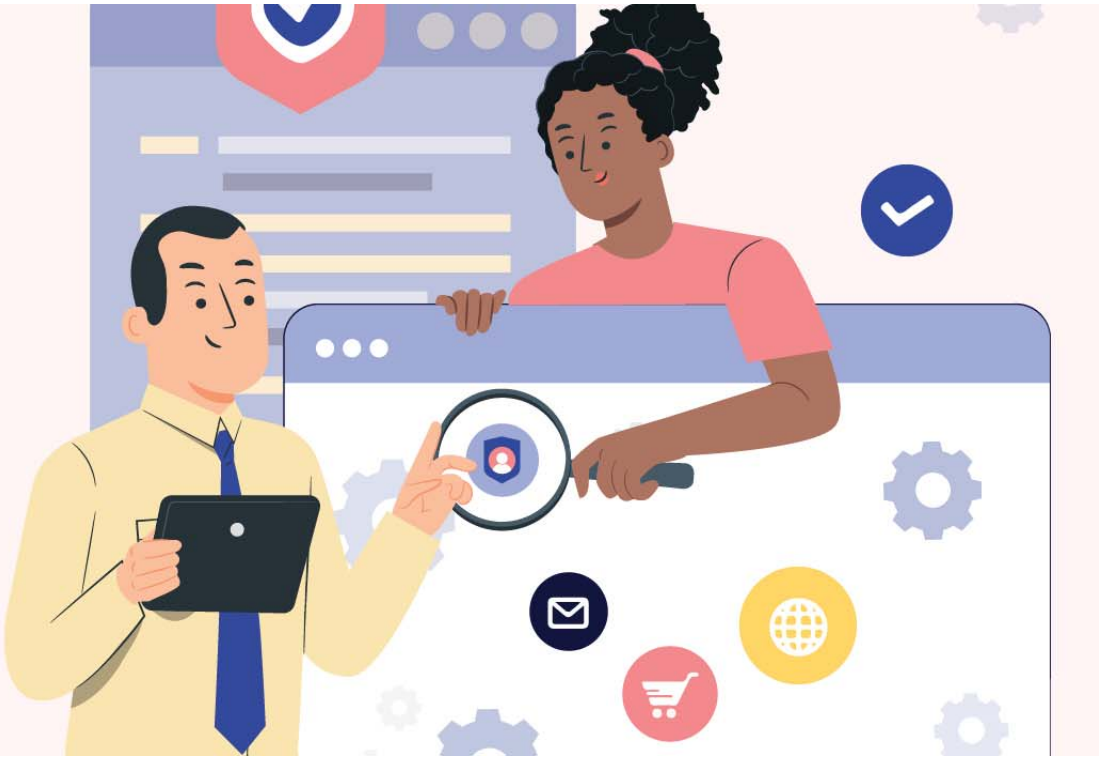
- **Não abrir** *emails* ou SMS, **nem clicar** em *links* ou anexos, desconhecidos
- **Não partilhar** informação profissional nas redes sociais ou *chats* e ser parco na partilha de dados pessoais
- Escolher as configurações de **privacidade** e **segurança** mais adequadas nas **videoconferências**: palavra-passe, fundo neutro, sala de espera, controlo de convidados, limpar o *desktop*, etc.

Cuidar dos dispositivos Em Viagem

- **Não carregar** equipamentos em **terminais públicos**
- Se tiver de se separar dos seus dispositivos, **retirar o cartão SIM** e, se possível, **a bateria**
- **Remover o histórico** das suas chamadas, registos e das páginas WEB
- **Desativar** a rede ***bluetooth*** enquanto viaja para evitar tentativas de ligação falsas

INTERNET SEGURA

#LerAntesClicarDepois



CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Necessidade de sensibilização da população

O número de incidentes registados pelo CERT.PT continua a aumentar de ano para ano, verificando-se um **crescimento de 14% em 2022** (de 1781 em 2021 para 2023 em 2022).

Este ano foi muito marcado por incidentes com efeitos particularmente disruptivos, bem como por um **aumento significativo no número de ataques de *ransomware*.**

O número de crimes da Lei do Cibercrime registados pelas autoridades policiais no ano passado cresceu face ao ano anterior, em 48%.

Em Portugal

Apesar de existirem várias organizações no país que realizam ações deste tipo, o uso dos meios de comunicação social de massas tem sido pouco frequente, em comparação com outros meios como as redes sociais, os cursos online ou as sessões presenciais.

Importância

A importância crescente deste tema e o aumento constante do número de incidentes e de cibercrimes, bem como a emergência de novos cenários de ameaças, justificam uma ação deste tipo.

Apresentação concreta da campanha

Esta campanha procura chegar ao maior número de pessoas possível com mensagens sobre as **boas práticas de ciber-higiene essenciais para a população.**

Serão lançados 21 vídeos dirigidos ao cidadão em geral, mas também ao contexto das organizações.

Ruth Ferrony
ruth.ferrony@cncs.gov.pt

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt | (+351) 210 497 400