DECO PROTeste

15 DE MARÇO 2024

DECO PROTeste

III CONGRESSO DIREITOS DO CONSUMIDOR

Cibersegurança

Perigo das ameaças digitais

Nota de contexto

A evolução das tecnologias da informação e comunicação beneficia milhões de pessoas que acedem a informação de diversa natureza.

A massificação da utilização de **correio eletrónico**, a **atividade online das empresas** ou a troca de informação através de **redes sociais** permite a transmissão de informação a uma escala sem precedentes.

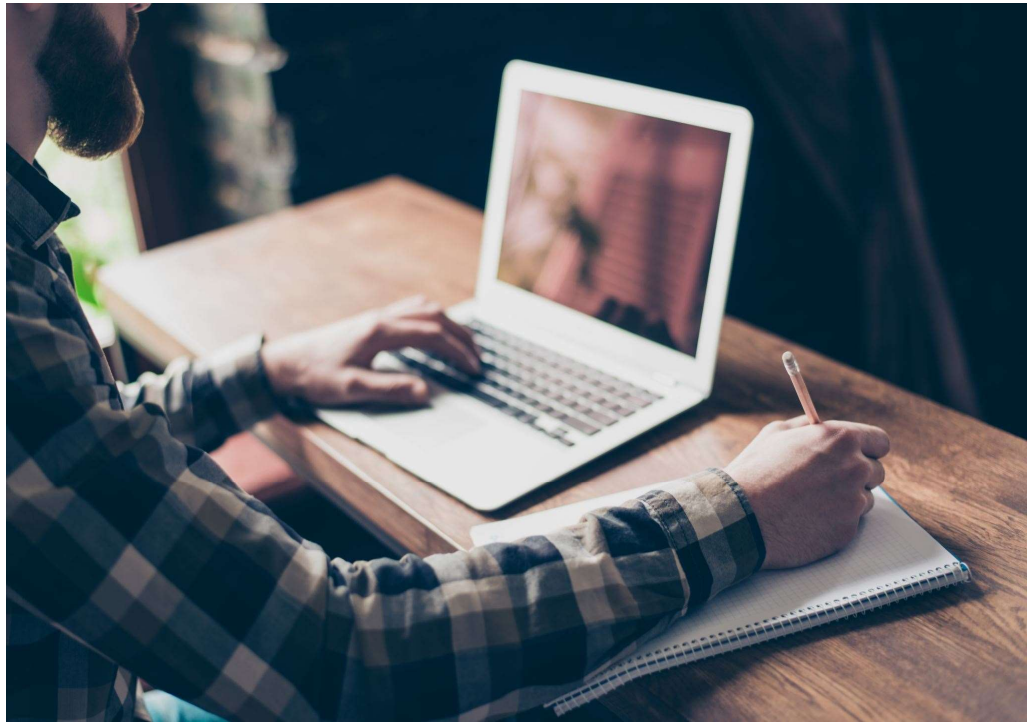
Estas vantagens podem representar um lado obscuro uma vez que o acesso a este tipo de informação também pode ser utilizada para finalidades ilícitas.

Novo quotidiano

- O confinamento implicou uma alteração de rotinas.
- Acréscimo significativo do **teletrabalho** e recurso generalizado de **compras online.**
- **Compras online**: consumidores podem adquirir bens em condições vantajosas.
- Empresas têm a possibilidade de **aumentar o volume de vendas**.

Procura incessante de alternativas para explorar novos hábitos adquiridos pelos consumidores através da criação de meios cada vez mais sofisticados para a prática de crimes.

Vulnerabilidade dos consumidores e das empresas



Ransomware

- **Ransomware:** bloqueio ou inviabilização de acesso a dados mediante um pedido de resgate para restabelecer o acesso.
- **Atividade criminosa** que ameaça os **cidadãos** e as **empresas.**
- **Principal dificuldade**: as medidas de proteção dos equipamentos nem sempre são eficazes.

Ransomware

- Os ataques podem afetar **setores vitais** da sociedade:

✓ **Transportes**
✓ **Energia**
✓ **Telecomunicações**
✓ **Saúde**

- Alguns ataques podem indiciar um tipo de **crime organizado.**
- A **investigação** e a obtenção de **prova pode ser complexa** e implicar a cooperação entre diversos países.

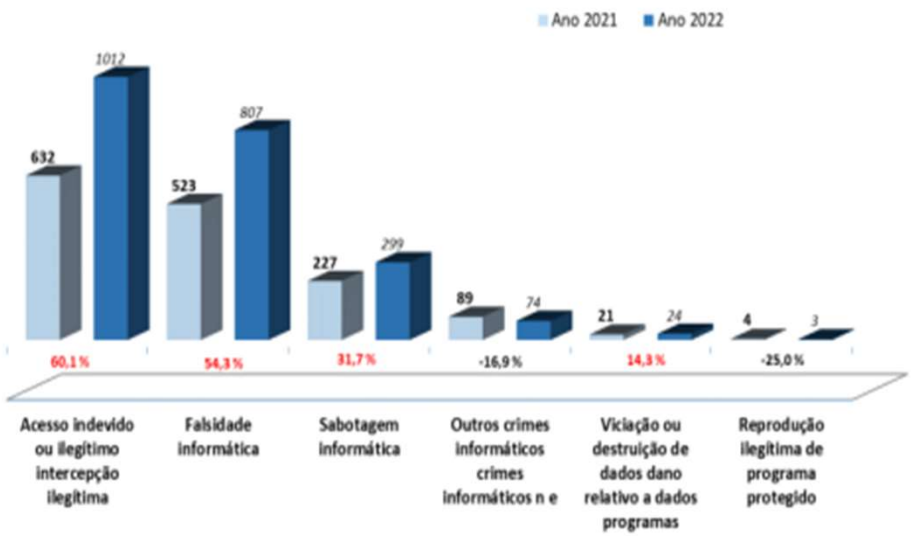

Sales
Sales plan
Weekly limit
Mothly limit
Annual limit
12%
12%
12%
12%
12%
100%
40%
Team C
Team D
Team E
Team A
Team B

DECO PROTeste

Relatório Anual de Segurança Interna

Aumento significativo dos crimes informáticos

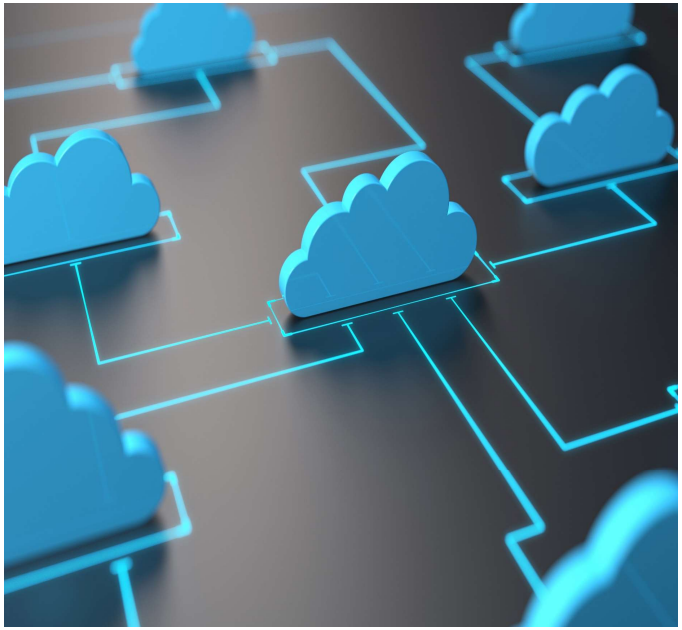
- Acesso ilegítimo
- Falsidade informática
- Sabotagem informática



Fonte: RASI 2022

DECO PROTeste

Lei n.º 109/2009, de 15 de setembro



Lei do Cibercrime

Lei n.º 79/2021, de 24 de novembro, procedeu à primeira alteração à Lei do Cibercrime.

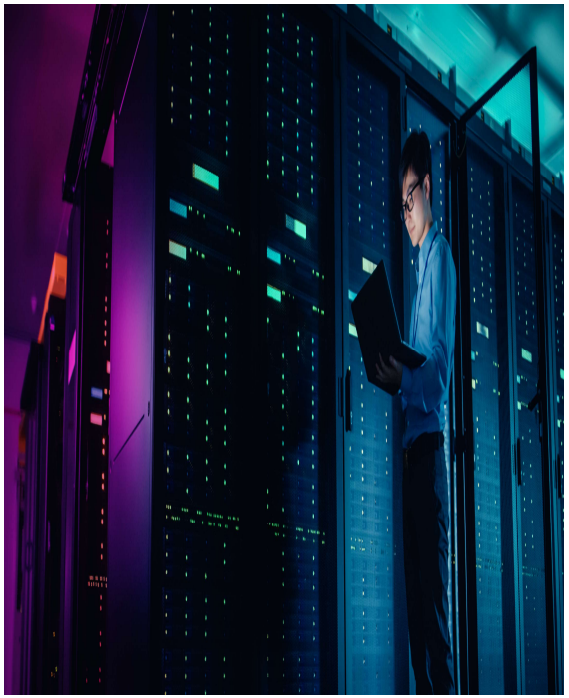
- Contrafação de cartões de crédito ou outros dispositivos de pagamento.
- Uso de cartões ou outros dispositivos de pagamento contrafeitos.
- Aquisição de cartões ou outros dispositivos de pagamentos contrafeitos.
- Aquisição de cartões ou outros dispositivos de pagamento obtidos mediante crime informático.

DECO PROTeste

Acesso ilegítimo

Artigo 6º

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo **aceder a um sistema informático**, é punido com pena de prisão até **1 ano ou com pena de multa até 120 dias.**
2 - Na mesma pena incorre quem ilegitimamente **produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir** num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, **um código ou outros dados informáticos** destinados a produzir as ações não autorizadas descritas no número anterior.
3 - A pena é de prisão até **2 anos ou multa até 240 dias** se as ações descritas no número anterior se **destinarem ao acesso para obtenção de dados registados, incorporados ou respeitantes a cartão de pagamento** ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.



DECO PROTeste

Acesso ilegítimo

Artigo 6º

4 - A pena é de prisão até **3 anos ou multa** se:

a) O acesso for conseguido através de violação de regras de segurança; ou

b) Através do acesso, o agente obtiver dados registados, incorporados ou respeitantes a cartão de pagamento ou a qualquer outro dispositivo, corpóreo ou incorpóreo, que permita o acesso a sistema ou meio de pagamento.

5 - A pena é de prisão de **1 a 5 anos** quando:

a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou

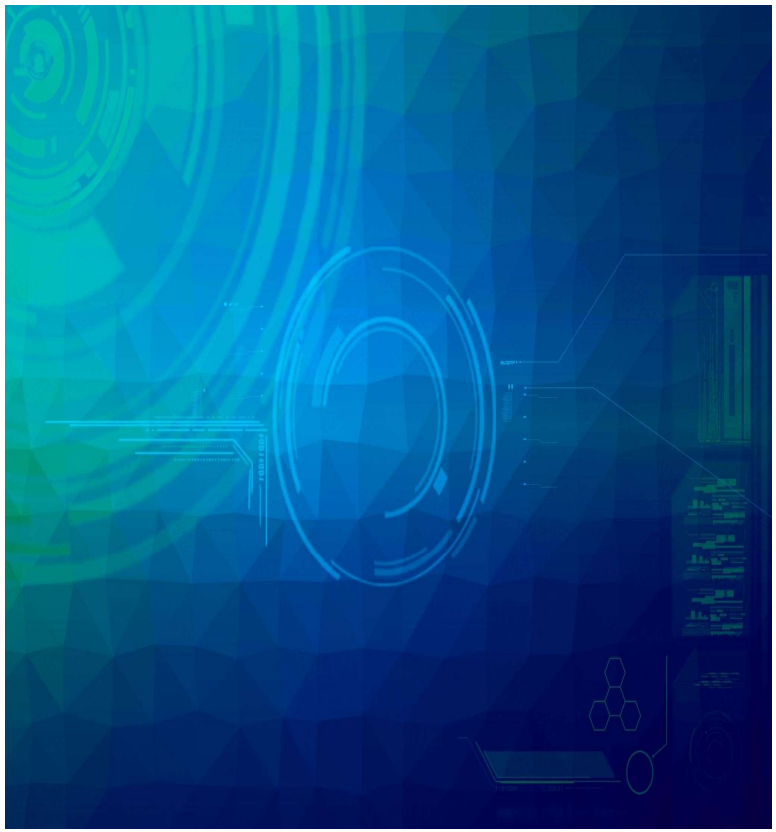
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

6 - A tentativa é punível, salvo nos casos previstos nos n.os 2 e 3.

7 - Nos casos previstos nos n.os 1, 4 e 6 o procedimento penal depende de queixa.

Acesso ilegítimo

- O acesso a uma rede social alheia, sem autorização, por terceiro que toma conhecimento de informação pessoal da vítima.
- A mesma conduta no acesso a uma conta de correio eletrónico.
- A utilização, sem autorização, de um acesso à Internet através de um serviço contratado a uma operadora de telecomunicações pela vítima.
- Ransamwere, na parte relativa ao acesso a dados informáticos de terceiro alheios.



DECO PROTeste

Falsidade informática

Artigo 3º

1 - Quem, com intenção de provocar engano nas relações jurídicas, **introduzir, modificar, apagar ou suprimir dados informáticos** ou por qualquer outra forma interferir num tratamento informático de dados, **produzindo dados ou documentos não genuínos**, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão **até 5 anos ou multa de 120 a 600 dias.**

2 - Quando as ações descritas no número anterior **incidirem sobre os dados registados, incorporados ou respeitantes a qualquer dispositivo que permita o acesso a sistema de comunicações ou a serviço de acesso condicionado**, a pena é de **1 a 5 anos de prisão**.

3 - Quem, atuando com intenção de **causar prejuízo a outrem ou de obter um benefício ilegítimo, para si ou para terceiro, usar documento produzido a partir de dados informáticos** que foram objeto dos atos referidos no n.º 1 ou dispositivo no qual se encontrem registados, incorporados ou ao qual respeitem os dados objeto dos atos referidos no número anterior, **é punido com as penas previstas num e noutro número, respetivamente.**

4 - Quem **produzir, adquirir, importar, distribuir, vender ou detiver qualquer dispositivo, programa ou outros dados informáticos** destinados à prática das ações previstas no n.º 2, é punido com pena de prisão de **1 a 5 anos**.

5 - Se os factos referidos nos números anteriores forem praticados por funcionário no exercício das suas funções, a pena é de prisão de **2 a 5 anos**.

DECO PROTeste

Falsidade informática

O phishing implica o envio de emails a diversos destinatários provenientes de uma suposta entidade legitima, por exemplo, Banco ou Autoridade Tributária, na tentativa de obtenção de dados pessoais: número de contribuinte, código de acesso a conta bancária, nº de conta bancária.

DECO PROTeste

Sabotagem informática

Artigo 5º

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, **entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático**, através da **introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos** ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até **5 anos ou com pena de multa até 600 dias**.

2 - Na mesma pena incorre quem ilegitimamente **produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos** destinados a produzir as acções não autorizadas descritas no número anterior.

3 - Nos casos previstos no número anterior, a tentativa não é punível.

4 - A pena é de prisão de **1 a 5 anos** se o dano emergente da perturbação for de valor elevado.

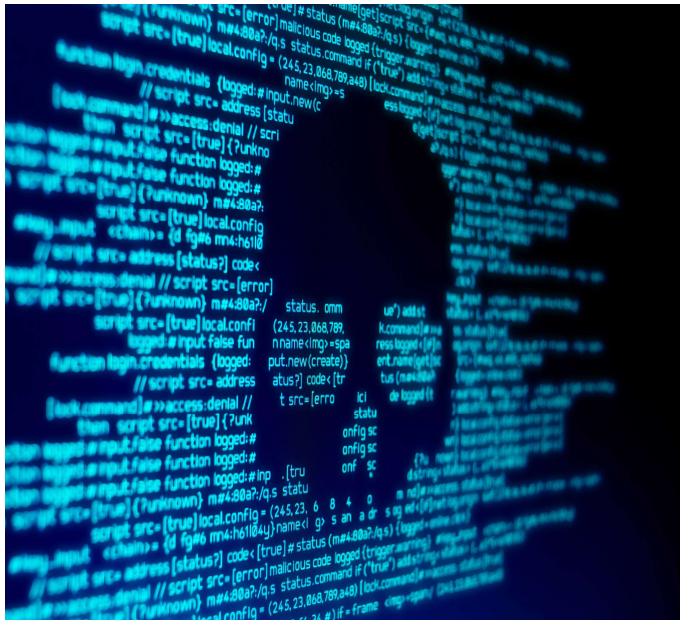
5 - A pena é de prisão de **1 a 10 anos** se:

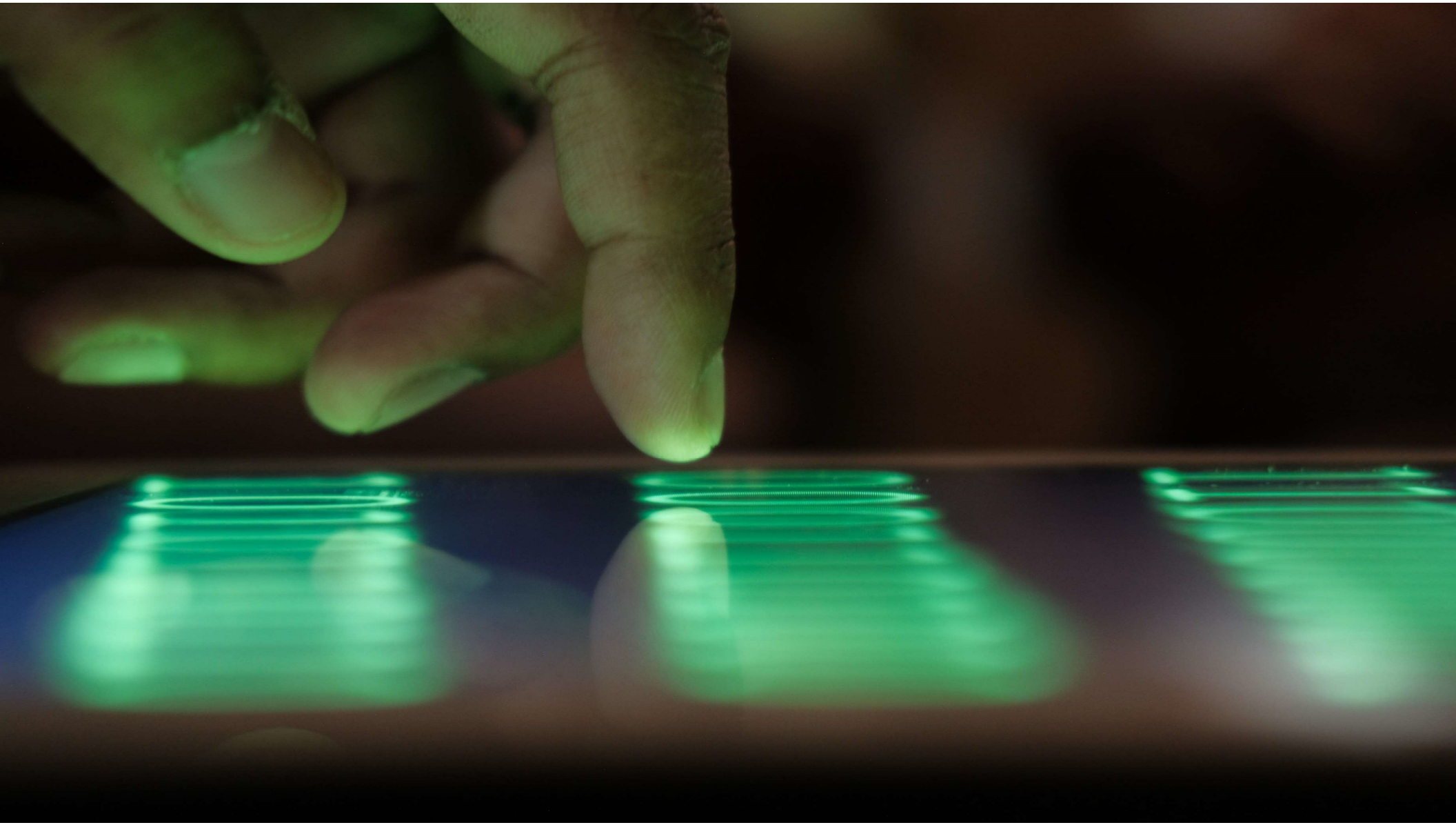
a) O dano emergente da perturbação for de valor consideravelmente elevado;

b) A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma **actividade destinada a assegurar funções sociais críticas**, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.

Sabotagem informática

Envio de vírus informático, um *Trojan Horse* com a finalidade de impedir, interromper ou perturbar com gravidade o funcionamento de um sistema informático.





Este site é seguro?

Identifica ameaças digitais

- Ajuda a determinar a segurança de um site.

- “Este site é seguro?” utiliza um algoritmo que fornece uma pontuação de confiança com base em diversas fontes de dados independentes, e em milhares de denúncias de sites maliciosos de entidades policiais, reguladores e organizações de defesa do consumidor de todo o mundo.

https://siteseguro.deco.proteste.pt/

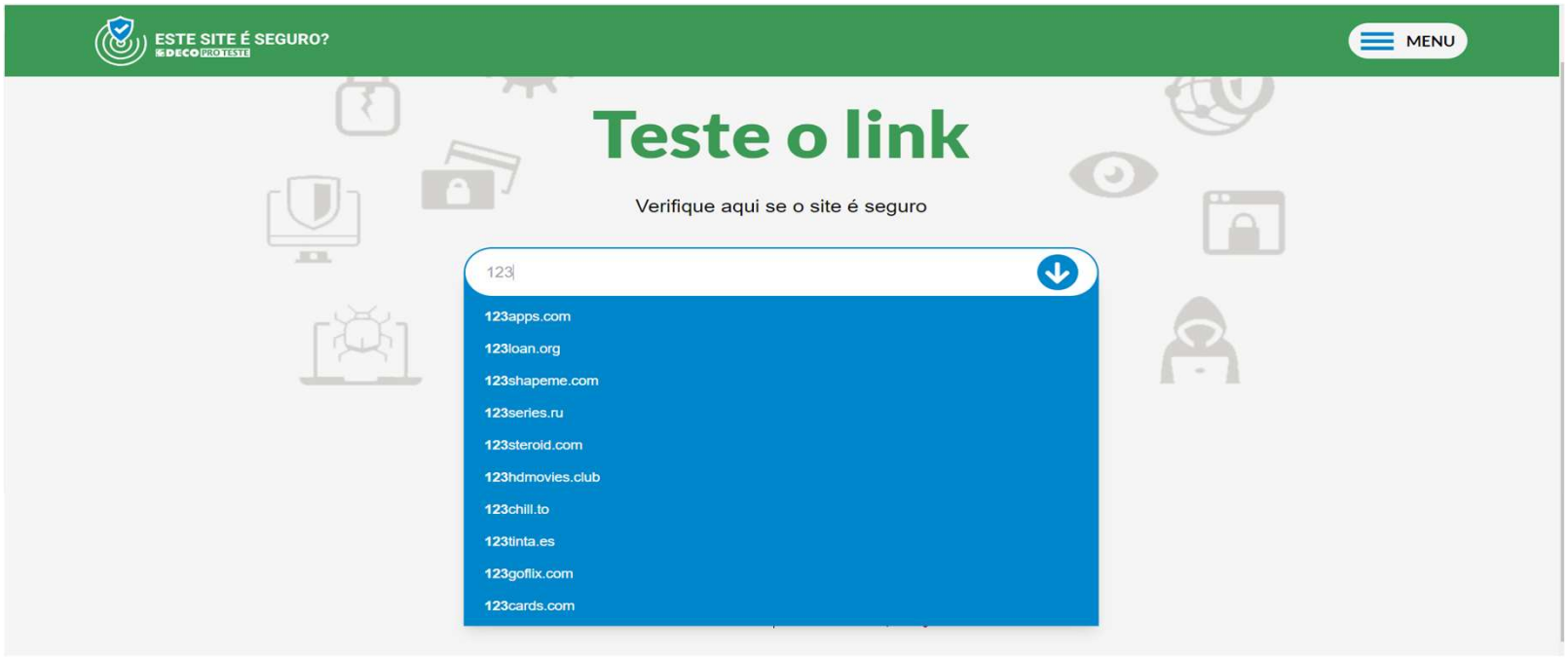
DECO PROTeste

Este site é seguro?

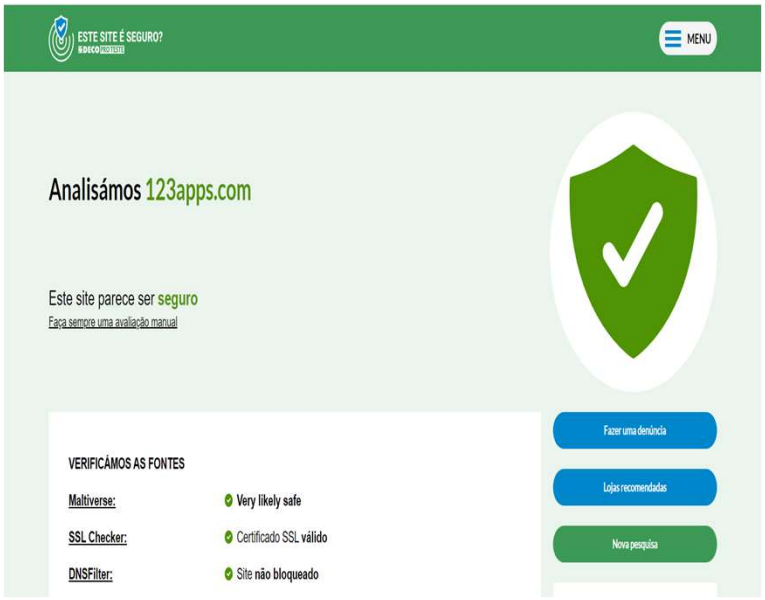
- “Este site é seguro?” foi projetado para fornecer informação sobre a segurança dos sites.
- Não classifica os sites com base na experiência de utilização dos consumidores: facilidade de navegação, questões relativas com a qualidade do serviço, prazos de entrega, devolução de bens ou elementos que não estejam relacionados com a segurança.
- Resultado da pesquisa: “Este site parece ser seguro”, significa que, em princípio, os consumidores não correm o risco de sofrer um cibercrime.

DECO PROTeste

Este site é seguro?



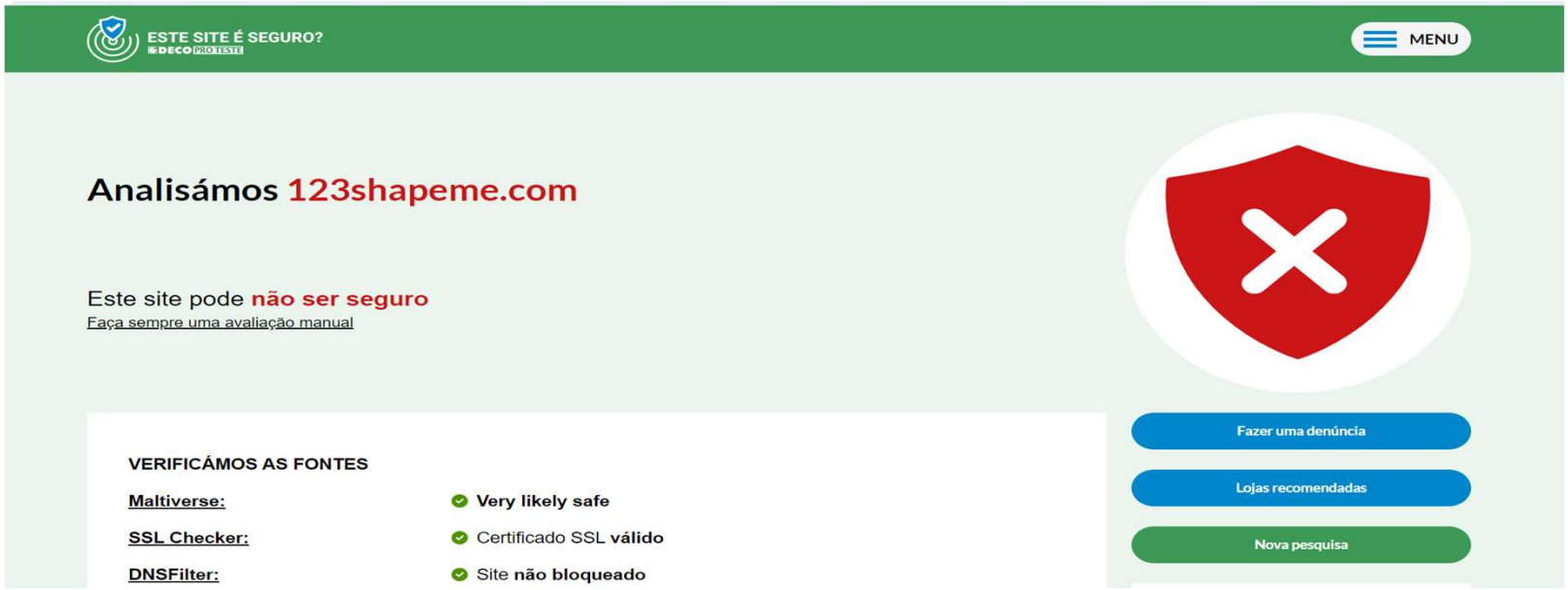
Este site é seguro?

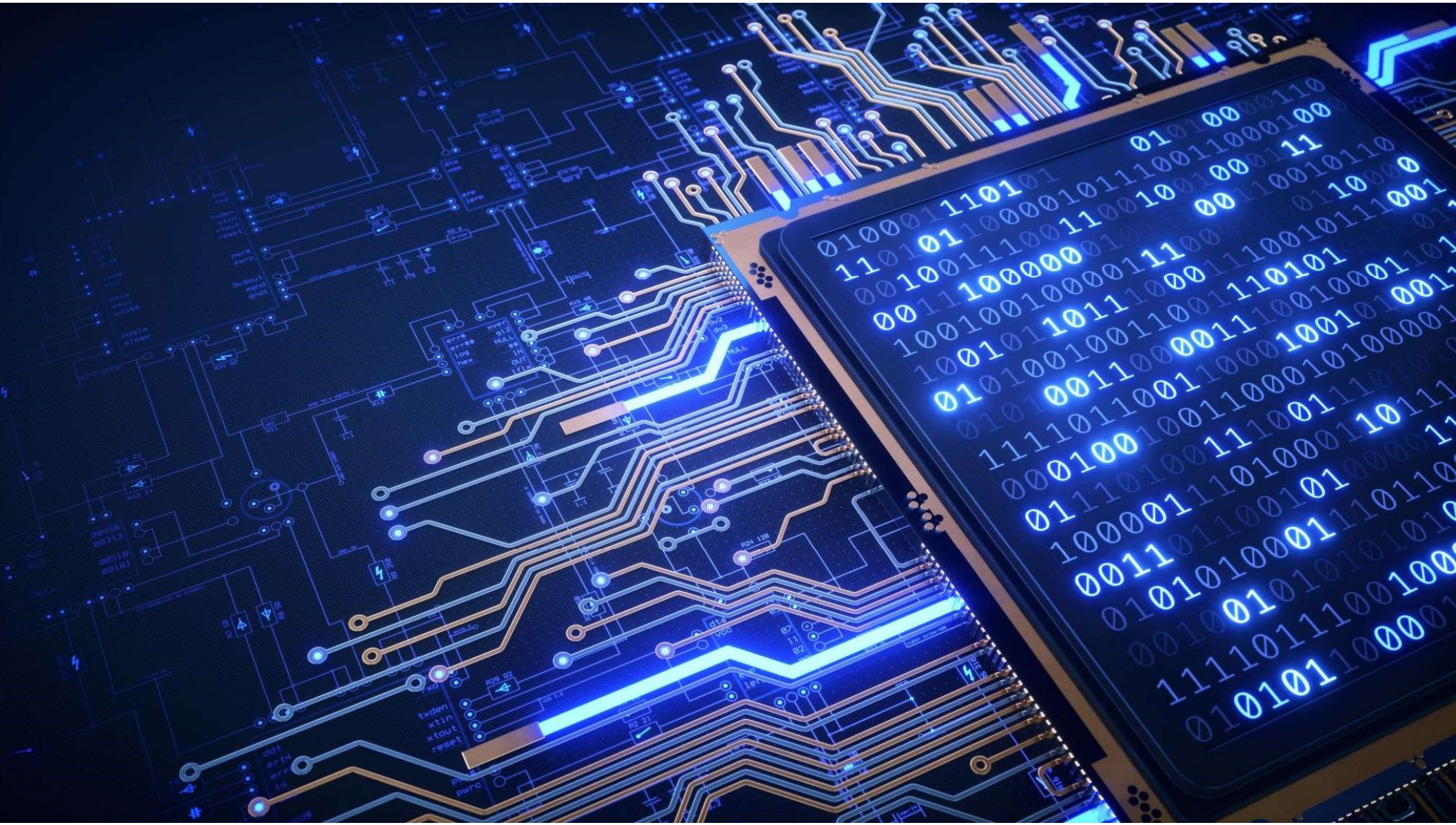


- **Dois resultados possíveis**: “Este site parece ser seguro” ou “Este site pode não ser seguro”.
- **Duas palavras chave:** “**parece**” e “**pode**” uma vez que nenhum dos resultados da pesquisa é definitivo.
- **Os resultados podem alterar à medida que novas informações são adicionadas** pelas fontes que alimentam o algoritmo.
- Exemplo: informações relacionadas com a infraestrutura do site, existência de protocolos de segurança, denúncias por vírus, phishing ou fraude.

DECO PROTeste

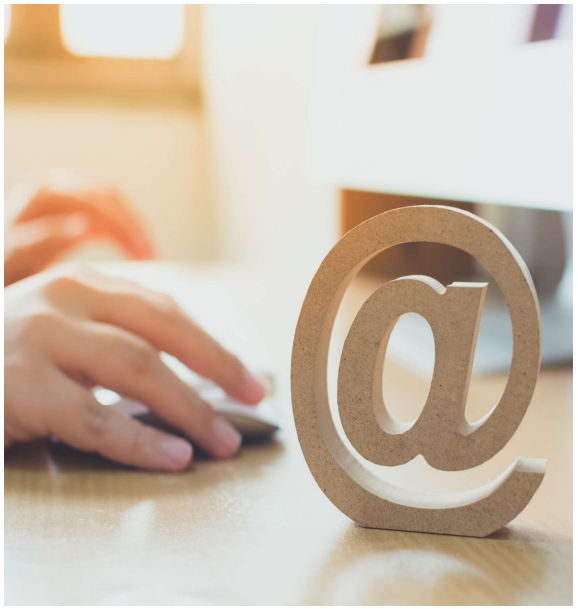
Este site é seguro?





DECO PROTeste

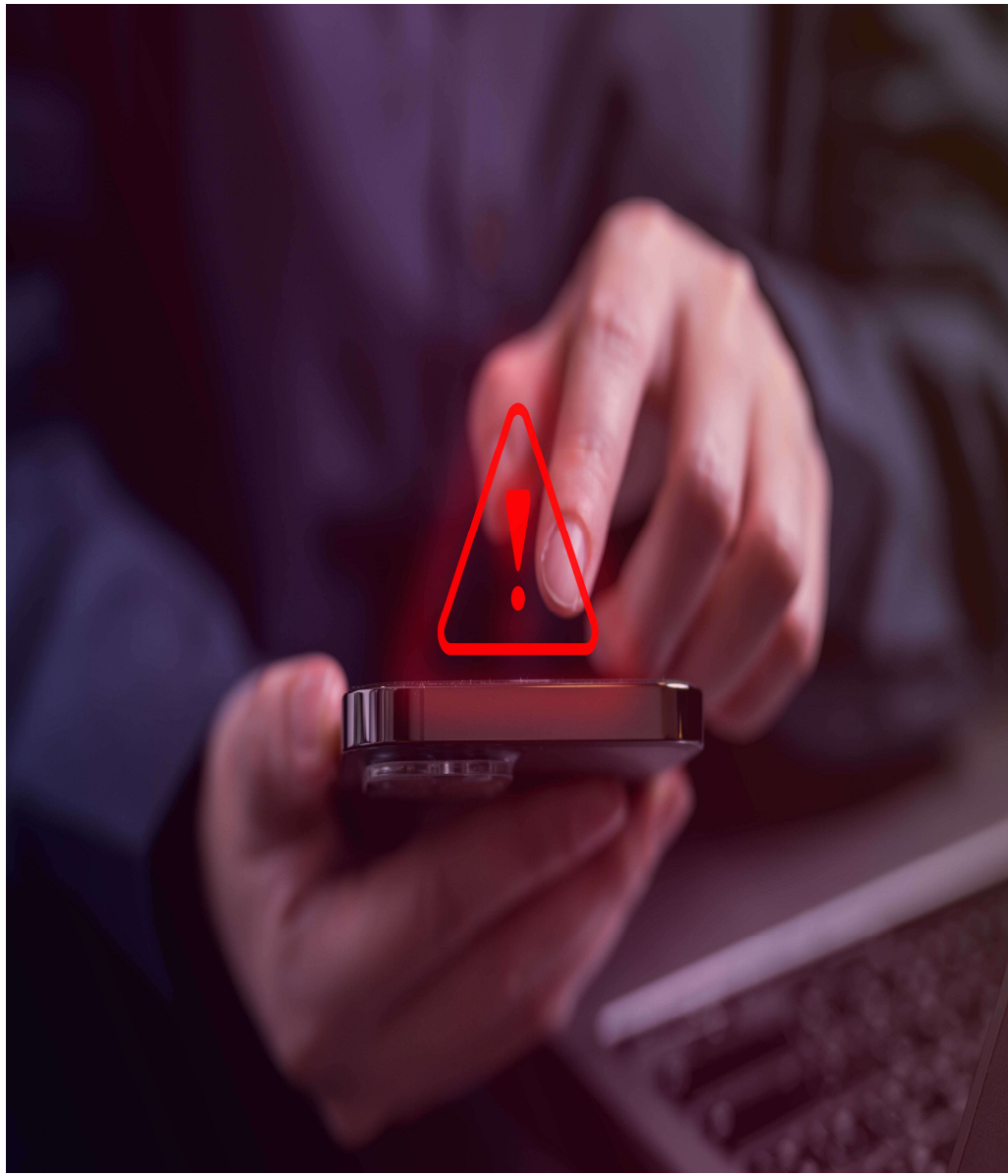
Como prevenir ataques informáticos



- Não clique num link ou anexo de email que não conhece
- Conta de correio eletrónico protegida com uma palavra-passe complexa
- Não usar a mesma palavra-passe para aceder diversos serviços
- Um gestor de passwords pode ajudar a gerir os diferentes acessos das contas e sugerir palavras fortes como alternativa
- Proteger o acesso às contas através de uma verificação em dois passos

Acesso ao banco

- Alterar com regularidade a palavra-passe.
- Atualizar o antivírus do computador.
- Não aceder ao site do banco através de links enviados por correio eletrónico.
- Digitar o endereço na barra do browser.
- Não abrir anexos de mensagens não solicitadas, mesmo que pareçam enviadas por conhecidos, o computador de um amigo pode estar comprometido e enviar e-mails malignos.
- Não partilhar o nome de utilizador, código de acesso ou cartão-matriz .
- Terminar a sessão depois de aceder ao site do banco.



SABER É PODER

DECO PROTeste

DECO PROTeste

top EMPLOYER PORTUGAL 2023
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Great Place To Work.
Certified
NOV 2022 - NOV 2023
PORTUGAL

DECO.PROTESTE.PT

218 410 858
Chamada para a rede fixa nacional
Dias úteis, entre as 9 e as 18 horas

AV. ENG. ARANTES E OLIVEIRA 13,
1900-221 LISBOA