PSafe

Crimes virtuais durante a pandemia:
o aumento dos vazamentos e ataques no Brasil

psafe.com

Crimes virtuais durante a pandemia:
o aumento dos vazamentos e ataques no Brasil

Cenário atual: uma pandemia de ciberataques feitos com I.A.

Em 2021, identificamos três megavazamentos de dados no país:

- **+223 milhões** de CPFs expostos em janeiro
- **40 milhões** de dados de empresas, incluindo CNPJ, razão social e data de fundação
- **+100 milhões** de contas de celulares expostas em fevereiro
- **+426 milhões** o maior vazamento de informações sensíveis de pessoas e empresas, expostas em um site público em setembro

Vazamento de dados é um problema global

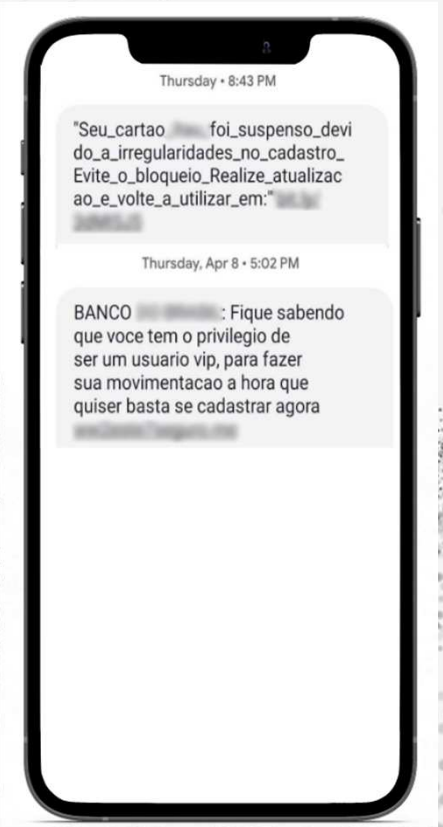
E a ciberpandemia segue crescendo...

Golpes têm muitos canais de acesso e riscos enormes

- Normalmente esses golpes são disseminados por links e/ou programas maliciosos;
- Os principais canais de disseminação são: **redes sociais, WhatsApp, e-mail e SMS;**
- Entre os riscos estão **roubo de dados pessoais, financeiros e credenciais de acesso.**

Golpe Bancário

Golpe Bancário



Dicas de segurança:

1. Não clique e nunca informe dados pessoais em sites e apps de procedência desconhecida
2. Tenha uma solução de segurança que alerta e bloqueia estes golpes em tempo real.

E a grande ameaça desta ciberpandemia são os **RANSOMWARES**

Números alarmantes sobre os ataques de ransomware

US$ 20 bilhões

danos estimados pelos ransomwares em 2021 no mundo

11 segundos

tempo médio que leva para um novo ataque de ransomware ser registrado no mundo

97%

crescimento anual deste golpe

US$ 11 milhões

maior pedido de resgate que se tem notícia, pago pela JBS

3.8 milhões

número de ataques de ransomware registrados no Brasil somente em 2020

2º lugar

posição do Brasil no ranking dos países mais atacados por ransomware, ficando atrás somente dos EUA

US$ 570 mil

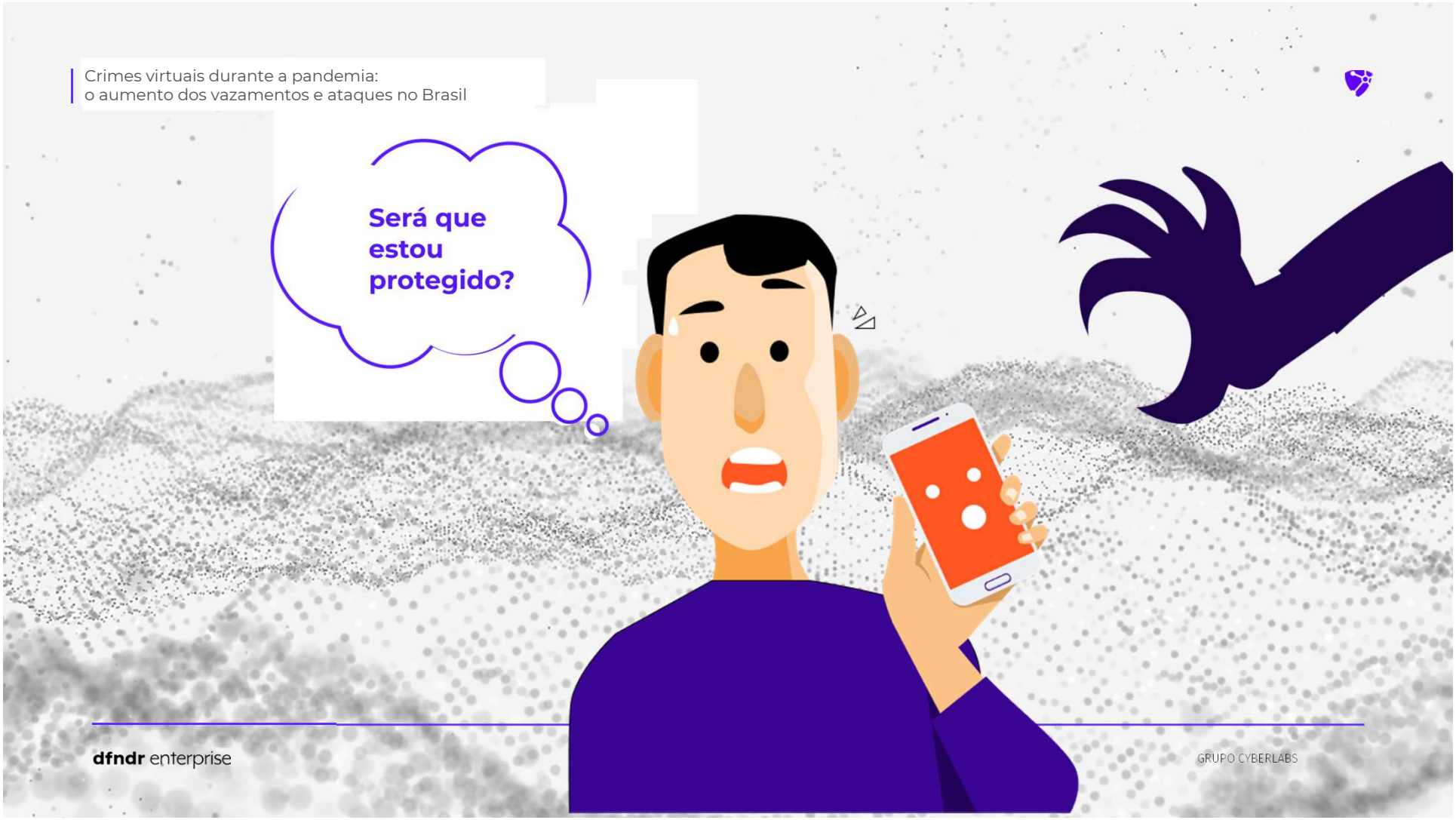
valor médio pago por organizações do mundo em resgates de ransomware

Como funcionam os ataques de ransomware

- Por meio de arquivos maliciosos, exploração de vulnerabilidades ou acesso remoto(seja por força bruta ou uso de credenciais vazadas) os criminosos **sequestram o acesso aos dispositivos e servidores da vítima.**

- Todos os dados dos sistemas infectados são criptografados pelos criminosos, que ameaçam só devolvê-los **mediante ao pagamento de um resgate.**

Crimes virtuais durante a pandemia:
o aumento dos vazamentos e ataques no Brasil



dfndr enterprise

GRUPO CYBERLABS

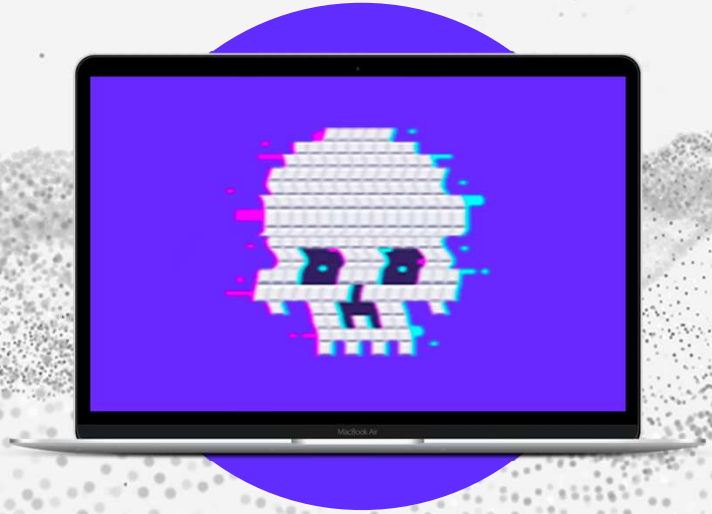
Como você lida com SENHAS?

Usa sempre a **mesma**

Muda apenas um caractere ou nenhum – o que coloca em risco a sua segurança.

Usa senha **fraca**

Sequências numéricas, aniversários e nome dos filhos são opções comuns e consideradas de baixa proteção.



Usa **senha de fábrica**

Os roteadores vêm com senhas alfanuméricas de fábrica, que já são conhecidas pelos hackers.

Dispensa 2º fator de autenticação

Esse código funciona como uma camada de proteção extra e seu uso dificulta a invasão de hackers.

As senhas mais utilizadas em 2020

Das 200 senhas mais utilizadas, “123456” foi a mais usada até 2020, com mais de 2,5 milhões de pessoas a escolhendo.

Esta é uma senha que leva menos de um segundo para ser hackeada, segundo a NordPass, uma empresa de gerenciamento de palavras-chave.

Utiliza alguma dessas? **Mude agora!**

123456	Senha
123mudar	Sucesso
Teste123	Vitoria
123123	Flamengo
111111	Password

Crimes virtuais durante a pandemia:
o aumento dos vazamentos e ataques no Brasil

Como você lida com a **CONEXÃO WI-FI?**

[O perigo das redes públicas e sem senha]

As redes Wi-Fi residenciais normalmente têm um nível de segurança inferior aos das redes corporativas.

É preciso proteger a sua conexão contra invasões, especialmente porque alguns ciberataques podem ser transmitidos a dispositivos conectados à mesma rede.

Devido à falta de proteção, redes públicas abertas e/ou sem senha podem ser um perigo para dados sensíveis.

Fonte: TechTudo / Dados: PSafe

Como você lida com APLICATIVOS?

[Hackers usam nomes de aplicativos conhecidos]

O “mercado de cibercrimes” não tem limites para atrair vítimas, e os hackers enxergaram uma grande oportunidade nos aplicativos, que atualmente são muito usados para facilitar ações do dia a dia. Por meio deles, os cibercriminosos espalham malwares e ransomwares.

Por isso, é essencial usar somente aplicativos baixados de fontes seguras (lojas oficiais), sempre ficar atento a quem são os desenvolvedores e comentários dos usuários.

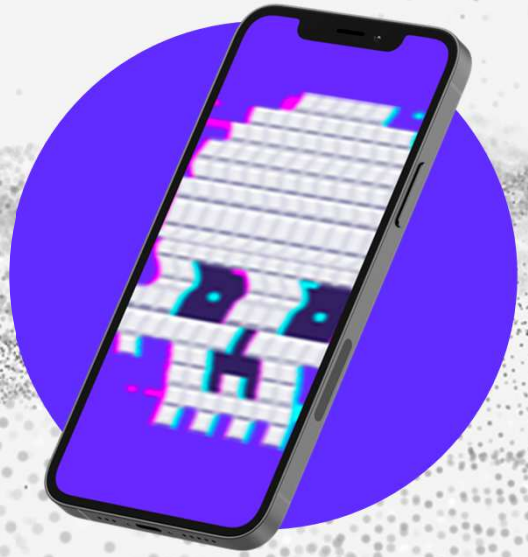
Como você lida com **DISPOSITIVOS PESSOAIS?**

Não verifico links antes de clicar

Links e sites maliciosos são um dos meios mais comuns para o roubo de informações.

Trabalho usando meu smartphone

O uso de um único aparelho para fins pessoais e profissionais facilita a ação de criminosos.



Acesso e-mails de trabalho

Basta uma credencial de acesso roubada e/ou vazada para que comunicações privadas e profissionais sejam expostas

Não uso um app de segurança

Hackers têm usado softwares sofisticados em seus ataques. Muitas ameaças só são detectáveis apenas com Inteligência Artificial.

LGPD: Nova regra para proteção de dados

Sanções e multas poderão ser aplicadas para empresas que violarem as normas sobre a coleta, tratamento e proteção de dados pessoais:

- Multa simples de até 2% do faturamento da empresa, de até R$ 50 milhões por infração;
- Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados;
- Suspensão parcial do funcionamento do banco de dados a que se refere a infração por até de seis meses, até a regularização da atividade.

A **prevenção** é um **investimento**.

A remediação gera um prejuízo que pode levar **à falência**.

** relacionadas a tratamento de dados vazados*

Obrigado

Visite nosso site

www.psafe.com

Contato PSafe:

Email: atendimento@psafe.com

PSafe