Segurança na Informática

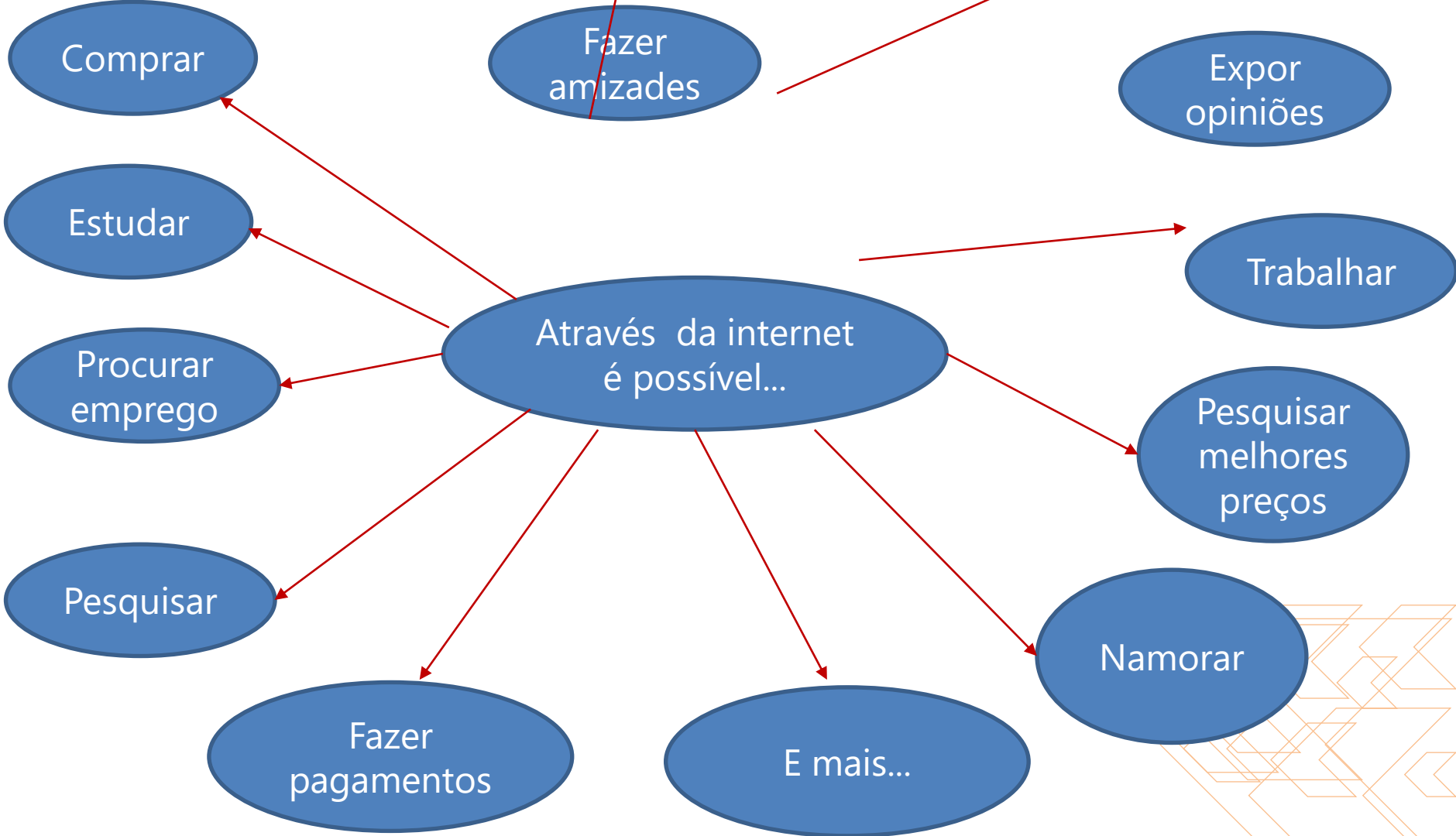
Prof. André Aparecido da Silva
Prof. Enzo A. Souza

A **segurança digital** é a prática de proteger sistemas, redes e programas de ataques virtuais. Esses ataques virtuais geralmente têm como objetivo acessar, alterar ou destruir informações confidenciais, extorquir dinheiro de usuários ou Interromper a continuidade dos negócios. Atualmente, a implementação de medidas de **segurança digital**

Tentamos nos resguardar de assaltos e mais recentemente, dos “caprichos” da natureza fazendo seguro de vida, seguro para o carro e para a casa, instalando redes de proteção, para-raio e cercas elétricas.

Mas não é só no mundo palpável que demanda cuidado.

Após a internet não conseguimos mais pensar na vida sem computadores, tablets, smartphones entre outros...


Através da internet é possível...
Comprar
Fazer amizades
Expor opiniões
Estudar
Trabalhar
Procurar emprego
Pesquisar melhores preços
Pesquisar
Namorar
Fazer pagamentos
E mais...

Tecnologia e Segurança

- Com o crescimento exponencial da internet e outras tecnologias de comunicação e interação cresce também os problemas derivados destas práticas.

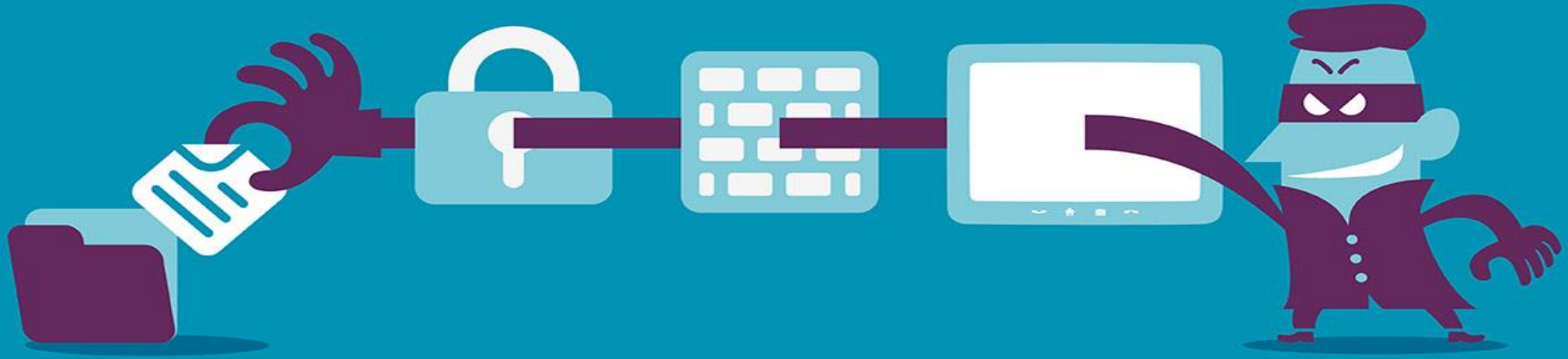
Tecnologia e Segurança

- Isto deve – se a falta de informação por parte dos usuários, também por sistemas sempre com alguma brecha de segurança ou por outros diversos motivos.

Por que invadir sistemas alheios?

Motivos para invadir

- Por meio da Internet você pode:
- Vandalismo;
- Pirataria;
- Ter acesso a informações privilegiadas;
- Uso do sistema computacional;
- Roubo de dados / informações;
- ....



Contato com pessoas mal-intencionadas

Existem pessoas que se aproveitam da falsa sensação de anonimato da Internet para aplicar golpes, tentar se passar por outras pessoas e cometer crimes como, por exemplo, estelionato, pornografia infantil e sequestro.

Furto de Identidade

Assim como você pode ter contato direto com impostores, também pode ocorrer de alguém tentar se passar por você e executar ações em seu nome, levando outras pessoas a acreditarem que estão se relacionando com você, e colocando em risco a sua imagem ou reputação.

Furto e perda de dados:

- Os dados presentes em seus equipamentos conectados a Internet podem ser furtados e apagados, pela ação de ladrões, atacantes e códigos maliciosos.

Invasão de privacidade

- A divulgação de informações pessoais pode comprometer a sua privacidade, de seus amigos e familiares e, mesmo que você restrinja o acesso, não há como controlar que elas não sejam repassadas.

- Além disto, os sites costumam ter políticas próprias de privacidade e podem altera-las sem aviso prévio, tornando público aquilo que antes era privado.

Dificuldade de exclusão:

- Aquilo que e divulgado na Internet nem sempre pode ser totalmente excluído ou ter o acesso controlado.

Dificuldade de manter sigilo

- Na Internet, caso não sejam tomados os devidos cuidados, as informações podem trafegar ou ficar armazenadas de forma que outras pessoas tenham acesso ao conteúdo.

Uso excessivo

- O uso desmedido da Internet, assim como de outras tecnologias, pode colocar em risco a sua saúde física, diminuir a sua produtividade e afetar a sua vida social ou profissional.

Keyloggers

- Um keylogger é um programa que consegue enviar para o hacker todas as teclas que você digita em seu computador. Assim, a senha é descoberta facilmente.

Tipos de vírus

- Trojan
- Macro
- Bot
- Spyware
- Ransomware

Keyloggers

- Atualmente, existem outros métodos que complementam o keylogger, permitindo o acesso a números de cartões de crédito e a senhas de redes sociais, e-mail, entre outros.

Screenloggers

- O keylogger não é mais tão eficiente para o roubo de informações bancárias porque boa parte dos bancos criou sistemas em que, ao invés de digitar a senha, o usuário precisa clicar em botões específicos.

Screenloggers

- Em contrapartida, os hackers criaram um software que captura toda a tela ao redor do mouse, oferecendo acesso a todos os cliques feitos pelo usuário.

Screenloggers

- Novamente, os bancos agiram trocando os botões de posição ou deixando o botão apagado no momento em que é clicado.

Screenloggers

- Os hackers criaram métodos para gravar em vídeo tudo o que o internauta faz e chegou-se à conclusão que a segurança feita pelos bancos ainda não era suficiente.

Como se previnir?

- Atualize os sistemas:

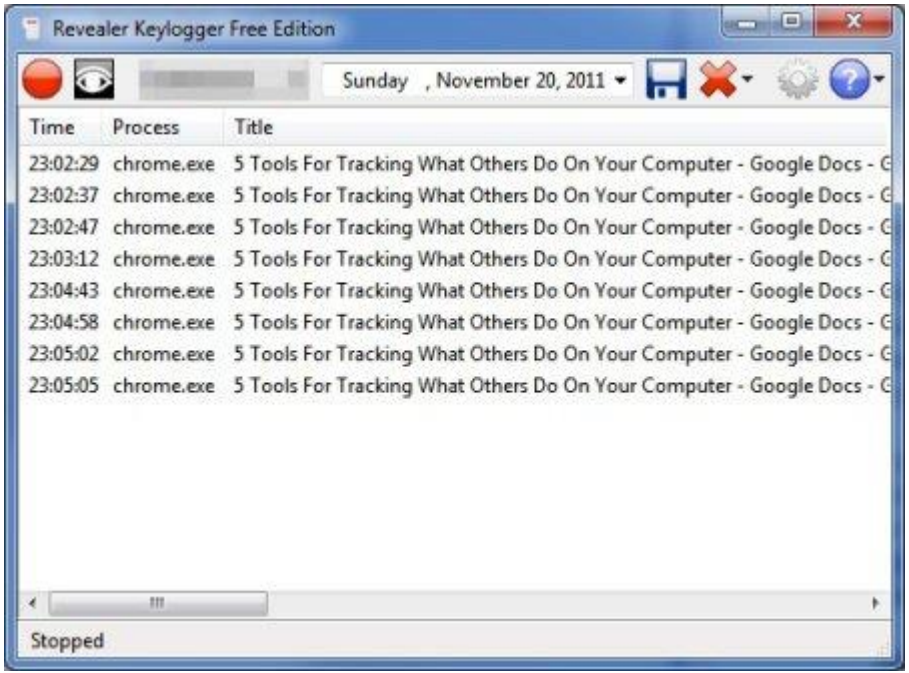
Use UM bom anti-virus

Faça Backup

Efetue logout ao sair

O logout significa se desvincular da sua conta.

NÃO GRAVE SENHAS NO COMPUTADOR



Use senhas boas

- No mínimo 10 caracteres;
- Mistura números e letras;
- Misture letras maiúsculas e minúsculas;
- Não sejam dados conhecidos;
- Misture caracteres especiais. Ex.: #@!*’-%_...

Use senhas boas

- Não use a mesma senha para tudo;
- Troque de senha regularmente. Ex.: Mês a mês;
- Associe a senha a algo fácil de lembrar;
- Não anote suas senhas no seus aparelhos eletrônicos, procure memorizá-las!
- Evite senhas relacionadas ao seu dia a dia. Ex.: data de nascimento ou casamento, nomes de familiares, ruas, trabalho, etc.

No celular

- Não deixe informações sigilosas, afinal é fácil perder o celular;
- Não deixe seu e-mail de uso pessoal logado.
- Use mecanismos de bloqueio para o celular;
- Não use senhas fáceis. Ex.: 1234, 159357, desenho de letras, ou até mesmo sem senha.

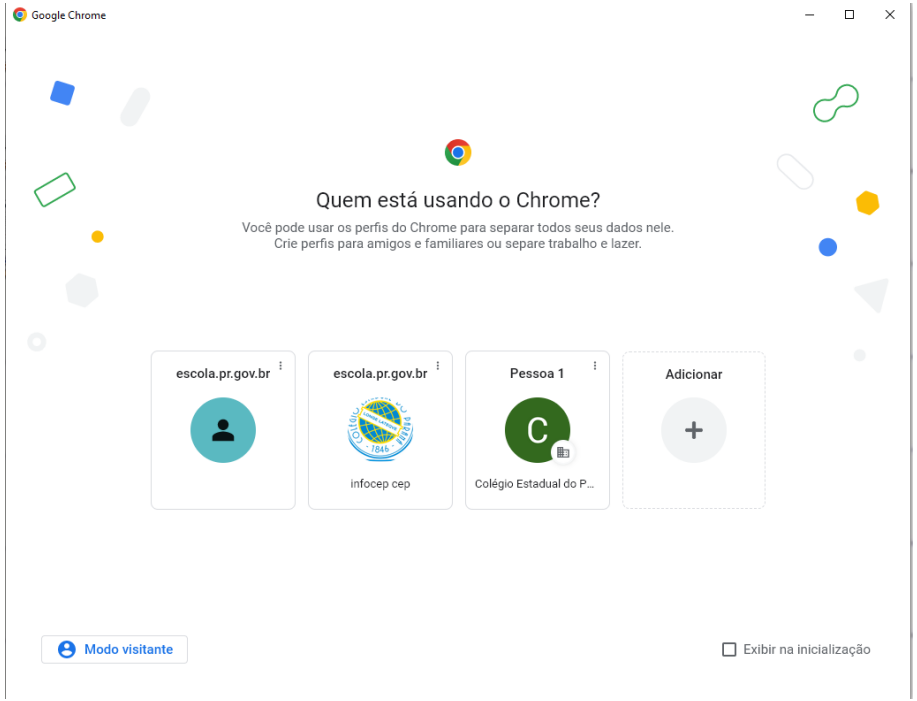
No celular

- Faça uso de recursos remotos.
- Configure aplicativos de segurança do celular.
- Faça a autenticação de 2 fatores.

Segurança no CEP

INFOCEP

Segurança no CEP

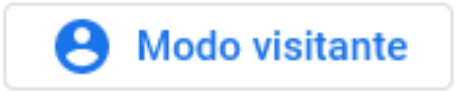


Usando o Google Chrome, ao ver essa tela, prefira sempre clicar em “modo visitante”.

Segurança no CEP

No modo visitante, como o próprio nome diz, você está apenas visitando!

O modo visitante impede que o Chrome salve suas atividades de navegação, incluindo:



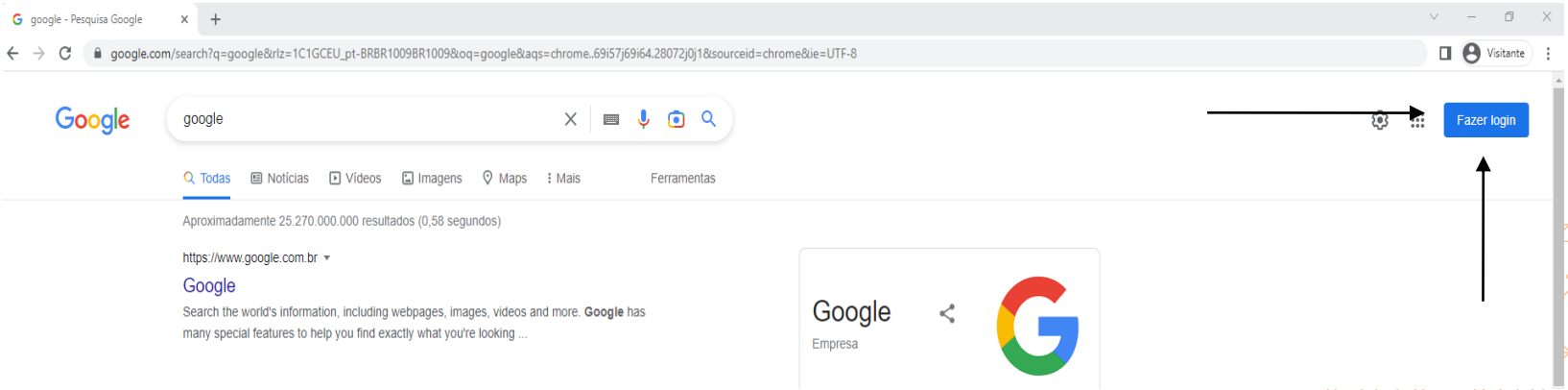
Segurança no CEP

Modo visitante

- Sites que você visita, incluindo os anúncios e recursos usados nesses sites
- Sites em que você faz login
- Seu empregador, escola ou quem administra a rede que você está usando
- Seu provedor de acesso à Internet
- Mecanismos de pesquisa
- Dados da sua conta

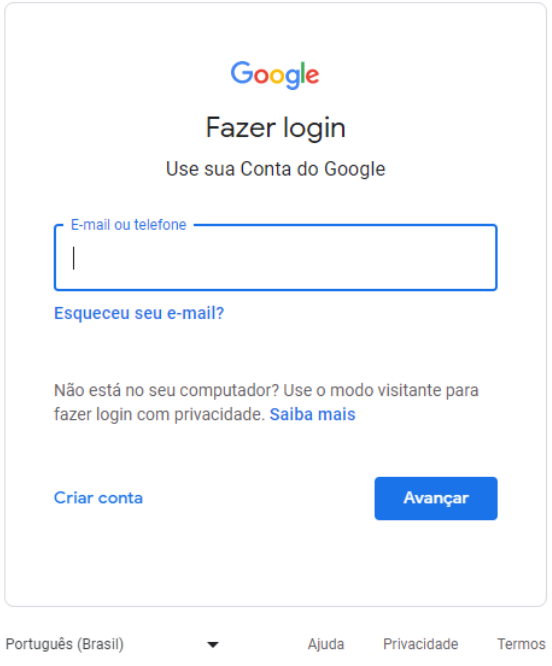
Segurança no CEP

Pesquise Google na barra de pesquisas e clique em “Fazer Login”.



Segurança no CEP

Faça seu login e use o Chrome normalmente durante sua aula.



Segurança no CEP

Ao término da aula, clique na sua foto de perfil, localizada no canto superior direito da tela, clique em “Sair” e certifique-se de que você fechou o navegador.

Segurança no CEP

Mais uma dica:

Ao usar o RCO, lembre-se de fazer o logout e fechar o navegador.
Assim o professor evita transtornos, como acessos desconhecidos e alteração de dados.

Extra!

Quer saber se seu e-mail, telefone e/ou senha foram comprometidos em algum vazamento de dados de alguma empresa grande?

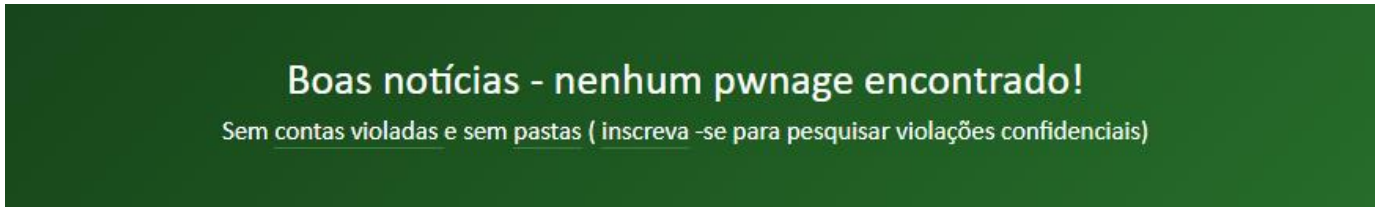
Acesse o site do folheto que você recebeu e digite seu e-mail ou telefone.

Extra!

Digite seu e-mail e dê um enter!

Extra!

Caso não tenha sido, você verá a seguinte mensagem em verde:



Extra!

Caso tenha sido, você verá a seguinte mensagem em vermelho, com todas as empresas e data do vazamento logo abaixo.

Extra!

Violações nas quais você foi preso

Uma "violação" é um incidente em que os dados foram expostos involuntariamente ao público. O uso do gerenciador de senhas 1Password ajuda a garantir que todas as suas senhas sejam fortes e exclusivas, de modo que uma violação de um serviço não coloque seus outros serviços em risco.

Animoto : Em julho de 2018, o serviço de criação de vídeo baseado em nuvem Animoto sofreu uma violação de dados . A violação expôs 22 milhões de endereços de e-mail exclusivos ao lado de nomes, datas de nascimento, país de origem e hashes de senhas salgadas. Os dados foram fornecidos ao HIBP por uma fonte que solicitou que fossem atribuídos a "JimScott.Sec@protonmail.com".

Dados comprometidos: datas de nascimento, endereços de e-mail, localizações geográficas, nomes, senhas

Aptoide : em abril de 2020, a loja de aplicativos Android independente Aptoide sofreu uma violação de dados . O incidente resultou na exposição de 20 milhões de registros de clientes que foram posteriormente compartilhados online por meio de um popular fórum de hackers. Os dados afetados incluíam endereços de e-mail e IP, nomes, endereços IP e senhas armazenados como hashes SHA-1 sem sal.

Dados comprometidos: detalhes do agente do usuário do navegador, endereços de e-mail, endereços IP, nomes, senhas

Obrigado!

Para quaisquer dúvidas, o INFOCEP fica à disposição no térreo, em frente ao RH.
Ramal: 5638