FIM DAS SENHAS:

em direção à um futuro **passwordless**

As senhas são parte integrante da nossa vida digital, protegendo informações mais sensíveis. Desde sua criação na década de 60, elas têm evoluído para se adaptar às crescentes ameaças cibernéticas.

Mas será que hoje elas são de fato a forma mais segura de autenticação no mundo virtual?

1. Cerca de **30 milhões** de senhas foram vazadas no Brasil em 2022.

2. Dentre as regiões com maior número de senhas vazadas, lideram a lista: **São Paulo** (18.666.801), **Rio de Janeiro** (9.237.689), **Minas Gerais** (1.122.777), **Paraná** (155.301) e **Rio Grande do Sul** (124.023).

3. **3.909.813** roubos de credenciais ocorreram através do browser Google Chrome no Brasil, segundo dados do **SafeLabs**, em parceria com a **ISH**.

4. **80%** das violações de segurança envolvem credenciais comprometidas.

5. O Brasil é o país com o **maior volume de dados expostos no mundo**.

CONHEÇA AS SENHAS MAIS UTILIZADAS PELOS BRASILEIROS E FUJA DELAS!

Na internet, as senhas fortes são as mais recomendadas para a proteção dos dados. Porém, as senhas padrão mais usadas pelos brasileiros são as fracas. Por isso, é importante entender a diferença entre elas para saber como se proteger.

Segundo um levantamento da ISH, 84,5% das senhas mais comuns no Brasil seriam quebradas por um hacker em menos de um segundo.

A clássica sequência "**123456**" segue liderando o ranking, não só no Brasil como em outros **41** países. Confira a lista:

- 123456
- 12345
- 123456789
- 102030
- Brasil
- senha
- 12345678
- 1234
- 10203
- 123123

O levantamento apresenta ainda que substantivos relacionados a comida, animais e grandes eventos também são comuns nas escolhas de senha dos brasileiros e devem ser evitados.

CAMINHOS PARA A PROTEÇÃO DAS SENHAS NO DIA A DIA

Em um mundo onde a nossa identidade digital e informações confidenciais estão constantemente sob ameaça, **proteger as senhas tornou-se mais crucial do que nunca**. Não são apenas as grandes corporações que são alvo; indivíduos e pequenas empresas também estão em risco.

Uma senha fraca diminui a segurança digital. Os riscos estão relacionados a golpes de roubo de identidade e financeiros, de informações e dados pessoais, facilitando o acesso criminoso a contas dos usuários.

Veja abaixo estratégias práticas e eficazes para fortalecer a proteção das suas senhas no dia a dia.

Crie senhas fortes

- **Complexidade:** Letras maiúsculas e minúsculas, números, símbolos, etc. Use combinações que façam sentido para você, mas que sejam difíceis para um computador adivinhar, como por exemplo:

8uF0ry4H_Rok$.

- **Únicas:** 58% dos brasileiros não trocam suas senhas com frequência. Reutilizar senhas pode comprometer várias contas. Crie uma senha única e original.
- **Tamanho:** Senhas com 12 ou mais caracteres são consideradas as mais seguras.

ADOTE AUTENTICAÇÃO DE DOIS FATORES OU APLICATIVOS MFA (MULTIFATOR):

As autenticações de dois fatores e MFA são processos de segurança que requerem que o usuário forneça duas ou mais formas de autenticação para acessar uma conta online. Ou seja, ela cria uma **camada de segurança adicional** para proteger a conta dos usuários contra acesso não autorizado, mesmo se a senha for comprometida.

1. **Importância:** Reduz o risco de invasão em 99,9%, segundo estudos.
2. **Tipos:** Mensagem SMS e e-mail, aplicativo autenticador, chave física (tokens ou cartões magnéticos).
3. **Uso:** Empresas que utilizam MFA têm menos chances de sofrer uma violação.

TENHA CUIDADO EXTRA AO ARMAZENAR AS SENHAS:

1. **Gerenciadores de Senha:** **Apenas 31%** das empresas usam algum tipo de gerenciador.

2. **Armazenamento Físico:** 42% das pessoas anotam senhas em papel.

3. **Evite salvar senhas em navegadores:** Grande parte dos roubos de senhas ocorrem através de browsers. De acordo com um levantamento da **ISH** em parceria com o **SafeLabs**, o Google Chrome foi o navegador que mais sofreu com roubo de informações armazenadas no Brasil. Ao todo, foram **3.909.813** credenciais vazadas. Em sequência estão o Microsoft Edge e Opera Browser, com **330.025** e **125.888** vazamentos, respectivamente.

4. **Cuidado com extensões maliciosas:** Um relatório da **ISH** alerta para a existência de diversas extensões maliciosas sendo disponibilizadas para download na Chrome Web Store, loja oficial do navegador. Somadas, as mais baixadas **ultrapassam 130 milhões** de downloads. São extensões que podem solicitar ao usuário o consentimento para **acessar sua localização, incorporação de anúncios** na Web, e **coleta de informações** (que, em casos maliciosos, podem se converter no roubo de dados de cartões de crédito e credenciais, por exemplo).

FIQUE ATENTO A INDÍCIOS DE VAZAMENTO:

1. **Monitoramento:** Utilize serviços de monitoramento de vazamentos.

2. **Alertas:** Um dado alarmante é que **40% das empresas não possuem alertas nem plano de contenção para vazamentos de dados**. Isso significa que, em caso de uma brecha de segurança, muitas organizações não têm os mecanismos necessários para **detectá-la rapidamente** e, consequentemente, não têm um **protocolo de ação** definido. Isso pode resultar em atrasos na resposta e, potencialmente, em danos maiores. Portanto, é essencial que as empresas invistam em **sistemas de alerta** e estabeleçam um plano claro de contenção para lidar com potenciais vazamentos.

3. **Ações Rápidas:** Altere senhas imediatamente em caso de suspeita.

RUMO A UM MUNDO SEM SENHAS?

O aumento de ameaças e ataques cibernéticos exige que as empresas busquem alternativas mais eficazes e convenientes para proteger suas informações sensíveis.

É dessa necessidade que surge o movimento **passwordless (sem senha)**. Estima-se que esse mercado deve movimentar aproximadamente **54 bilhões** de dólares até 2030, já que **as senhas sozinhas podem não ser suficientes.**

1. **Biometria:** Cerca de **85%** dos líderes globais pretendem recorrer à biometria como forma de autenticação segura.

2. **Autenticação Contínua:** Adotar monitoramento constante de padrões de uso e comportamento pode aumentar sua segurança.

3. **Mudança Cultural:** Estamos testemunhando uma verdadeira revolução na forma como as empresas veem a autenticação. A **tendência atual é a substituição gradual de senhas por outros métodos** mais seguros e convenientes de autenticação. Esta mudança cultural é impulsionada tanto pelo reconhecimento das vulnerabilidades das senhas tradicionais quanto pelo desejo de oferecer aos usuários uma experiência mais fluida e sem atritos.

O cenário do uso ou desuso das senhas está em constante transformação, com uma tendência rumo a métodos mais seguros de autenticação que possibilitam **mais proteção para usuários**. As práticas de segurança de hoje não refletem apenas necessidades do presente, mas também ajudam você a se preparar para o futuro digital, avanços tecnológicos e ameaças emergentes.

INOVAÇÕES EM SEGURANÇA DE SENHAS E ACESSO

A ISH conta com soluções **robustas** e **abrangentes**, visando garantir que apenas as pessoas certas tenham acesso às informações certas no momento certo.

ISH Board AM: O ISH Board AM é um sistema para **criar, armazenar e gerenciar identidades** de usuários e permissões de acesso com segurança, através das funcionalidades: gestão de autorização, múltiplo fator de autenticação, criação de logon único, autenticação e detecção de login suspeitos.

Os casos de uso de AM se expandem para **acesso interno** (identidades da força de trabalho, incluindo, mas não limitado a funcionários, trabalhadores temporários, terceirizados e contratados) e casos de uso de **acesso externo** (incluindo clientes, parceiros, cidadãos e talentos freelance contingentes).

ISH Board PAM: O ISH Board PAM é uma solução de **gerenciamento de acesso privilegiado de nível empresarial** que pode ser implantada rapidamente e facilmente gerenciada. Com o Secret Server, você pode descobrir e gerenciar automaticamente suas contas privilegiadas por meio de uma interface intuitiva, protegendo contra atividades maliciosas em toda a empresa.
As funcionalidades da solução incluem:

1. **Gerenciamento de Credenciais:** Permite controlar de maneira eficaz e segura todas as credenciais privilegiadas.
2. **Descoberta de Privilégios:** Identifica automaticamente contas e acessos de alto privilégio, simplificando o processo de administração.
3. **Cofre Seguro:** Armazena as informações sensíveis de forma protegida, garantindo que apenas usuários autorizados tenham acesso.
4. **Delegação de Acesso:** Facilita a distribuição de privilégios de maneira controlada e conforme as necessidades da equipe.
5. **Controle de Sessões:** Oferece monitoramento em tempo real e controle sobre as sessões privilegiadas em andamento.

QUER SABER MAIS? ENTRE EM CONTATO COM A ISH

Garanta que a segurança da sua empresa esteja alinhada com os padrões modernos.