01/02 - Dia Mundial de Mudar sua Senha: saiba como criar combinações seguras

Especialistas em segurança da Dock dão dicas e apontam erros mais comuns; não é seguro, por exemplo, utilizar a mesma combinação para todos os acessos

São Paulo, 31 de janeiro de 2022 - 1° de fevereiro é o Dia Mundial de Mudar sua Senha. A data foi criada para chamar a atenção dos usuários de tecnologia sobre a importância de alterar as combinações usadas para acessar e-mails, redes sociais, aplicativos, dispositivos e programas.

Os brasileiros lideram o ranking dos países que passam mais horas por dia no celular, segundo relatório da plataforma AppAnnie. O país passou das 4,1 horas diárias em 2019 para 5,2 horas diárias em 2020, até chegar às 5,4 horas diárias em 2021.

"Com vidas cada vez mais conectadas e o acesso virtual diário a uma série de plataformas que contém nossos dados pessoais - bancos, gerenciadores de fotos, planos de saúde, ferramentas de trabalho etc -, a segurança online precisa ser uma preocupação, já que o que os hackers buscam é uma vulnerabilidade", afirma Fred Amaral, co-founder da Dock, uma das empresas líderes na América Latina em tecnologia para serviços financeiros.

Para colaborar com este propósito, especialistas em segurança da Dock reuniram dicas e boas práticas para criar e manter senhas seguras, dificultando a atuação de invasores:

- Priorize a complexidade. É comum que tentativas de invasão aconteçam por meio de "bots", robôs automáticos que tentam realizar login durante horas. Quanto mais complexa a senha, mais tentativas são necessários e mais provável que o sistema bloqueie o invasor
- Não utilize seu nome, data de nascimento, cidade, telefone ou sequências fáceis como "1234".
- Utilize em torno de 10 caracteres. Caso o sistema exija menos ou mais, use variações, inserindo ou retirando caracteres especiais e números
- Use uma frase ou combinação de palavras não óbvias e que não seja fácil de ligar a você com uma busca em suas redes sociais. Uma frase de música, por exemplo, é mais difícil de relacionar a você do que o nome do seu animal de estimação. Os hackers procuram em seus perfis termos para usar nos bots como ponto de partida

- Você pode criar um “tronco principal” e inventar variações em cima dele. Troque letras por números parecidos, como “A” por “4” e “i” por “1”, além da “a” por “@”. Por exemplo:

#M4c4colouc07391 - E-mail
#Maca_cocrazy0682 - Instagram
#M@c@codo1d0_0573 - Facebook

- Evite a tentação de usar a mesma senha para todos os acessos a fim de facilitar a memorização. Utilize “cofres de senhas”, que são gerenciadores de acessos que as mantêm em um único local de forma segura, como o LastPass, o 1Password e o Bitwarden
- O padrão de segurança que as empresas seguem para troca de senha é geralmente a cada 3 meses. Para uso pessoal, a recomendação é que seja feita, no mínimo, a cada 6 meses
- Ative recursos de duplo fator de autenticação, que enviam sms ou solicitam códigos acessíveis em aplicativos para cada acesso
- Verifique se suas senhas foram vazadas no site haveibeenpwned.com, que mostra também se outros dados pessoais seus foram descobertos. É possível realizar cadastro para ser avisado caso outro incidente aconteça

Para os usuários que já possuem uma série de senhas e querem aumentar a segurança, a Dock recomenda começar pelas mais importantes, como as de bancos, email e redes sociais.

Roubo de senhas

A Dock explica que existem duas principais formas utilizadas por hackers para roubar senhas: por meio de bots (robôs), que adivinham a senha realizando centenas de tentativas de combinações por minuto, muitas vezes com base em informações sobre a vítima encontradas na internet; ou enganando o usuário por meio de sites falsos ou mensagens que solicitam login e senha.

Na maioria dos casos, o objetivo é de ganhos financeiros, obtidos diretamente de contas de banco, pedindo resgate de um perfil de rede social roubado ou enviando mensagens fingindo ser o dono do perfil ou número de celular.

Caso detecte um vazamento, roubo ou tentativa de roubo de sua senha, troque-a imediatamente e, se outras plataformas utilizarem a mesma senha, altere também. Se a senha for de banco, informe a instituição. Verifique também o registro de logins e sessões ativas do aplicativo e, caso encontre um acesso desconhecido, desconecte imediatamente.

Web 3.0

A web 3.0 transformou praticamente todas as redes em "plataformas" às quais aplicativos podem se conectar para acessar dados de usuários. Internautas começaram a adotar, como rotina e em um único clique, a prática de compartilhar senhas com esses serviços, deixando de avaliar os riscos de conectar esses aplicativos aos perfis de redes sociais. O compartilhamento da senha, processo extremamente arriscado, foi reduzido a um único passo.

Sobre a Dock

A Dock é uma das líderes na América Latina em tecnologia para serviços financeiros e a primeira em Banking as a Service na América Latina. Atualmente, viabiliza mais de 160 milhões de contas e processa mais de 50 bilhões de dólares em pagamentos anualmente. A companhia agrega inovação e escalabilidade aos negócios de seus clientes, reunindo Emissão de Cartões, *Digital Banking* e Soluções de Adquirência em uma plataforma única, além de Soluções de Risco & *Compliance*.

As soluções da Dock facilitam processos que aceleram a capacidade de empresas criarem serviços de meios de pagamento e de *digital banking*. O resultado é um leque amplo de produtos inovadores, maior acesso de consumidores a serviços financeiros e uma melhor jornada do cliente final.

A plataforma em nuvem da Dock reduz o encargo operacional e regulatório de seus clientes, ao mesmo tempo que oferece ferramentas valiosas ao negócio por meio de seu ecossistema de parceiros. A intenção é reduzir o *time-to-market* dos seus clientes.

Para mais informações, visite dock.tech

Contato - Assessoria de Imprensa Dock
Stephanie Milate
(11) 9-9240-5718
stephanie.milate@dock.tech