# Full Duplex Authentication®

## Mitigação de phishing e ataques Browser-in-Browser e de proxy malicioso

Este documento apresenta Full Duplex Authentication®, uma tecnologia de segurança projetada para enfrentar as ameaças crescentes de phishing, navegador dentro do navegador e proxy malicioso. Para compreender Full Duplex Authentication®, analisaremos primeiro essas ameaças e depois a abordagem inovadora da patente dos EUA 11,245,526.

## Introdução

A segurança on-line é essencial diante da evolução das ameaças digitais. Phishing e ataques Browser-in-Browser e de proxy malicioso são métodos usados para comprometer credenciais e informações confidenciais. Full Duplex Authentication® se apresenta como uma solução robusta para combater essas ameaças.

## O que é autenticação?

Autenticação é o processo de verificar uma identidade digital on-line. Quando uma pessoa está associada a uma identidade digital, ela fornece credenciais para comprovar que é quem afirma ser.




Três métodos comuns de validação:

- O primeiro é algo que o usuário sabe: uma senha, um número de identificação pessoal (PIN) ou um código de uso único (OTP).

• O segundo é algo que o usuário possui, como um dispositivo registrado, um token digital nesse dispositivo ou um equipamento físico específico, como uma YubiKey.

• O terceiro é algo que o usuário é: uma característica biométrica, como rosto ou impressão digital. Quando o usuário executa mais de uma ação de verificação, trata-se de autenticação multifator (MFA). Para garantir o mais alto nível de segurança ao autenticar uma identidade digital, os três métodos devem ser executados a cada autenticação em um sistema ou serviço.

## Ameaças à autenticação

**Engenharia social e phishing causam 70% a 90% das violações maliciosas.**

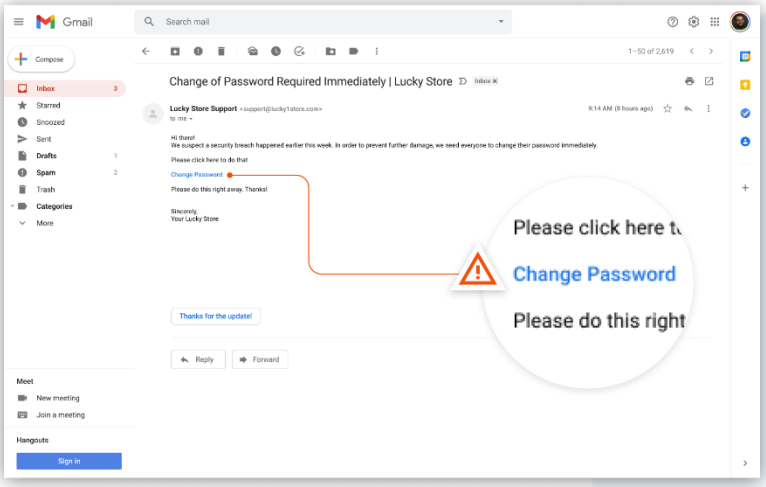
Fonte: KnowBe4

Há anos, os invasores concentram seus ataques no roubo de credenciais de acesso on-line.

Segundo o Verizon DBIR, em 2023, 74% das violações de segurança envolveram o elemento humano, incluindo ataques de engenharia social, como phishing.

Obter credenciais por engenharia social tornou-se mais fácil para os invasores do que realizar ataques sofisticados de força bruta.

Estes são alguns métodos comuns para obter credenciais de forma fraudulenta e contornar a autenticação multifator:

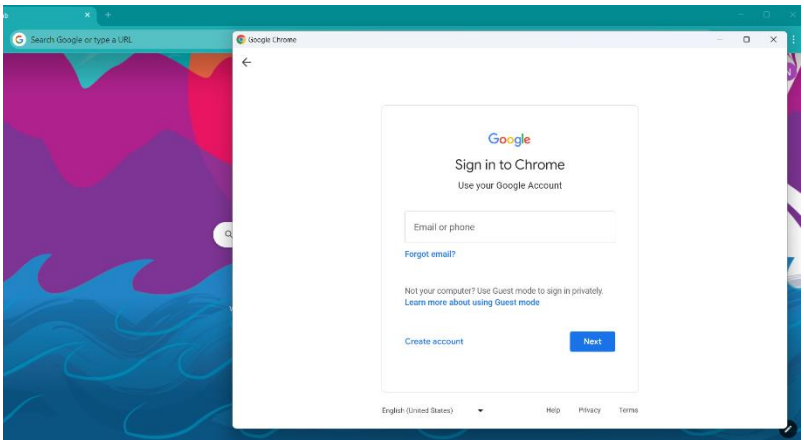



• Phishing: tentativas fraudulentas de obter informações confidenciais fingindo ser uma entidade confiável. Geralmente se espalha por e-mails ou sites falsos e explora a psicologia humana para induzir a divulgação de dados. Inclui smishing, por mensagens de texto, e vishing, que ataca redefinições de senha enviadas por correio de voz. Quishing usa códigos QR para conduzir a vítima à armadilha. O phishing costuma combinar e-mails e sites com identidades falsas.

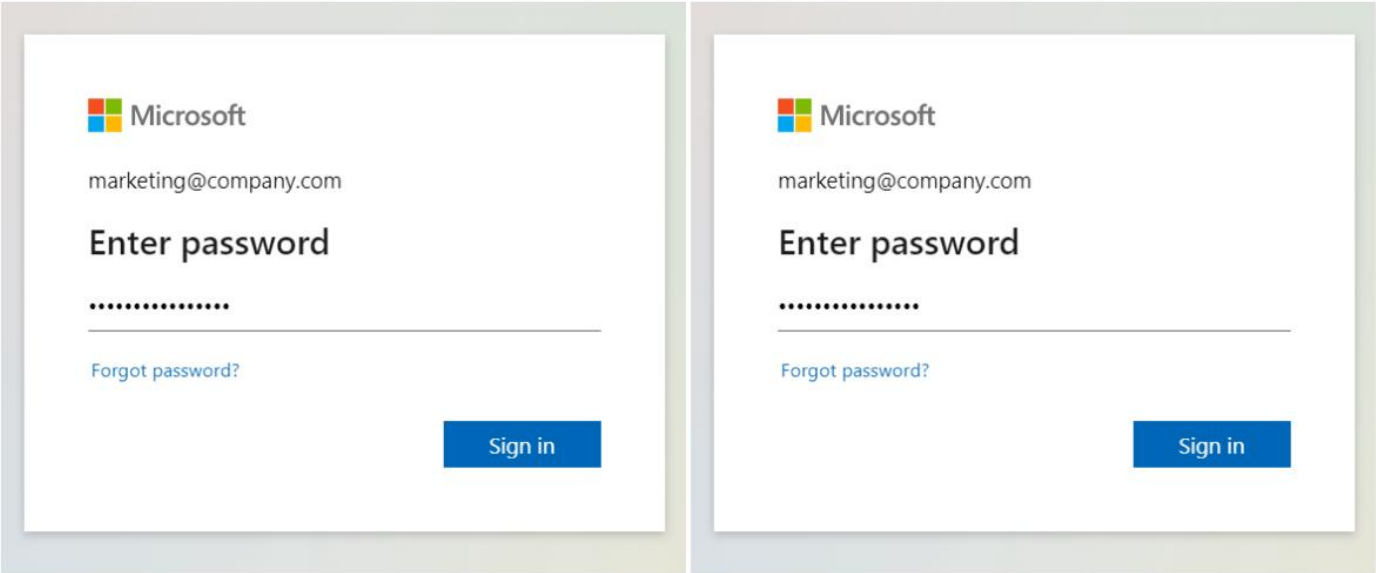
O usuário recebe um e-mail falso que parece vir de uma organização legítima, como

um banco, uma operadora de telecomunicações ou Amazon, Microsoft, Apple ou Google. O e-mail informa um problema na conta e pede login. Ao clicar no link, o usuário pode não perceber que a URL difere do site esperado. Quando insere suas credenciais, a conta é comprometida.

• Ataques Browser-in-Browser: uma entidade maliciosa injeta código em um site legítimo e compromete a segurança do navegador. Pode roubar informações confidenciais ou executar ações não autorizadas em nome do usuário. O ataque é difícil de detectar: o usuário pode não notar a mudança de URL porque as caixas de diálogo de navegador dentro do navegador não exibem uma URL. Ao inserir as credenciais, sua conta é comprometida.




• Ataques de proxy malicioso: interceptam a comunicação entre o usuário e o servidor web por meio de proxies maliciosos. Os invasores podem interceptar dados confidenciais, manipular a comunicação e roubar a senha durante o login.




Você consegue identificar o que é falso?

## Sobre Full Duplex Authentication®

Mesmo que se abandonassem os métodos baseados em conhecimento, isso não impediria os ataques atuais de phishing e engenharia social. Segundo este documento, os métodos de autenticação têm uma falha fundamental: o fluxo de verificação é unidirecional. O serviço solicitante desafia o usuário a executar as ações necessárias para comprovar sua validade.

O usuário também deve poder exigir que o serviço de autenticação comprove sua validade. Caso contrário, invasores podem se passar por um serviço legítimo para obter a senha, um token digital ou a verificação biométrica do dispositivo. A Identité® desenvolveu e patenteou Full Duplex Authentication® para tratar essa falha. A patente dos EUA 11,245,526 descreve um método com comunicação bidirecional e criptografada entre o usuário e o sistema. Diferentemente da autenticação unidirecional convencional, Full Duplex Authentication® mantém uma troca contínua e dinâmica de informações em todo o fluxo de autenticação.

## Como funciona Full Duplex Authentication®?

Um servidor de autenticação chamado NoPass™ pela Identité, abreviação de «sem senha», cria uma relação segura com um serviço de terceiros. O serviço coleta a identificação do usuário e inicia a autenticação. Pode ser Microsoft AD ou Azure, ferramentas SSO como Okta, VPN, Citrix ou qualquer aplicativo ou portal que exija autenticação. NoPass™ oferece várias formas de integração. • SSO federado: o servidor NoPass™ atua como provedor de identidade para Microsoft Azure/AD ou outras ferramentas SSO, como Okta, PingIdentity e KeyCloak. • RADIUS: o servidor NoPass™ é configurado




como cliente RADIUS.

• API: o servidor NoPass™ estabelece comunicação segura com portais web e aplicativos móveis.

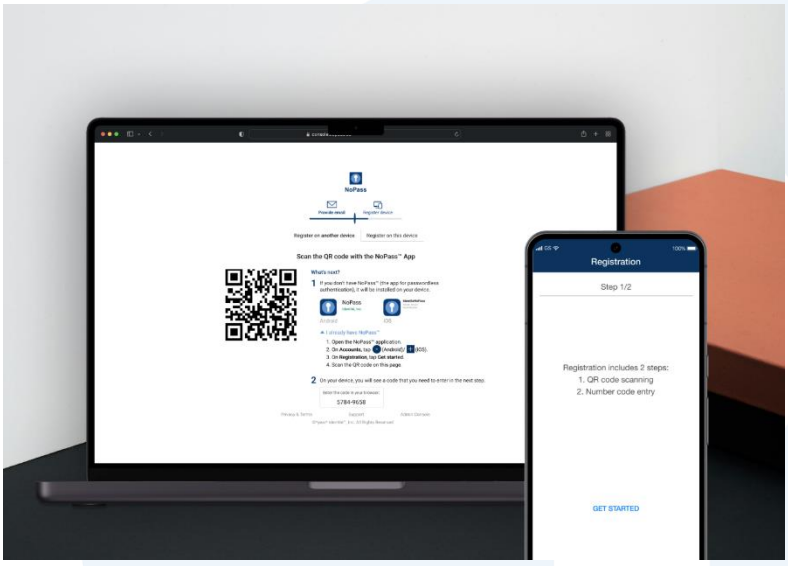
O servidor NoPass™ interage com o usuário por aplicativos para iOS, Android, Windows e macOS, disponíveis nas lojas públicas, normalmente no primeiro cadastro. O aplicativo recebe notificações push seguras quando o usuário solicita autenticação em um servidor de terceiros configurado para usar NoPass™ Full Duplex Authentication®. Ele contém credenciais exclusivas para cada portal ou serviço cadastrado. Elas são criptografadas e não podem ser reutilizadas para acessar um serviço, por exemplo em um ataque de repetição. Os usuários podem fazer backup e sincronizá-las com outros dispositivos se a política permitir.

## Cadastro no Full Duplex Authentication®

Para se cadastrar, o usuário se autentica pelo fluxo nativo do serviço, normalmente com nome de usuário e senha. Após a verificação, ele é redirecionado à interface de cadastro do Full Duplex Authentication®. O cadastro envolve o usuário e um dispositivo, como PC, Mac ou smartphone.

Conforme a política de segurança do servidor de autenticação NoPass™, o usuário escolhe o dispositivo e instala um pequeno aplicativo. Ele armazena uma credencial Full Duplex Authentication® para cada conta do usuário em cada serviço cadastrado. São aceitas várias contas no mesmo serviço.

A interface de cadastro permite ler um QR code ou tocar ou clicar em «Continuar», abrindo a instalação local do aplicativo Full Duplex Authentication®.

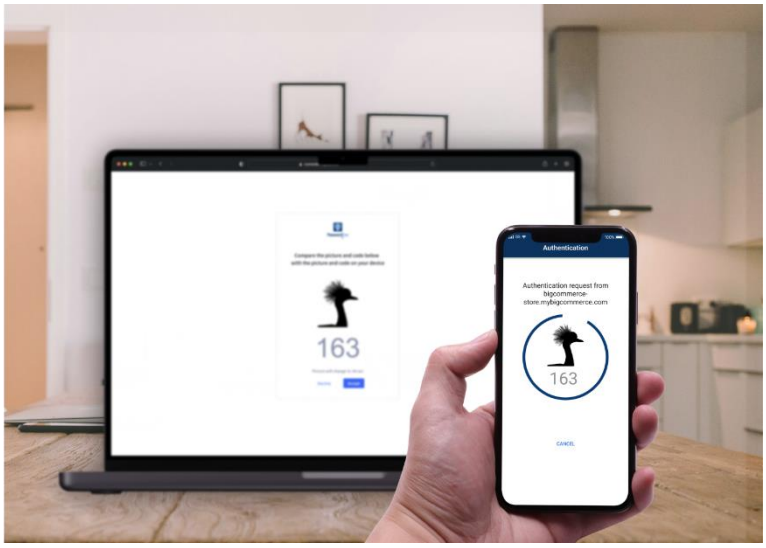



Se o aplicativo for instalado em um dispositivo diferente daquele que mostra o cadastro, o usuário confirma um código de oito dígitos para comprovar a posse do segundo dispositivo. Após a confirmação do cadastro, ele é autenticado e retorna ao serviço para continuar a tarefa. Quando sai e retorna, nenhuma senha é solicitada: ele segue o fluxo de Full Duplex Authentication®.

O aplicativo Full Duplex Authentication® reconhece e utiliza os fatores adicionais disponíveis no dispositivo, como biometria e tokens físicos YubiKey. Também pode ser configurado um PIN. Esses fatores adicionais reduzem os riscos em caso de perda ou roubo do dispositivo.

## Fluxo de uso do Full Duplex Authentication®

O usuário pode escolher um ou dois dispositivos. Dois dispositivos oferecem mais segurança: um exibe o diálogo de login e o segundo, com o autenticador, recebe e aceita a notificação push. O usuário inicia o login informando seu nome no primeiro dispositivo. O nome é enviado ao NoPass. Se estiver registrado, o NoPass envia instruções ao portal cadastrado. Ao inserir o nome de usuário, uma imagem e um número aparecem no dispositivo de autenticação registrado.




Full Duplex Authentication® se completa quando o aplicativo do dispositivo registrado autentica o servidor e aceita a mensagem para mostrar a imagem e o número. Ao aceitar as credenciais do servidor, o aplicativo descriptografa e reproduz a mesma imagem e número no dispositivo de autenticação. Eles mudam a cada 30 segundos; o processo se repete até o usuário responder. As configurações do NoPass podem limitar as tentativas para evitar que o usuário aceite uma notificação por fadiga de push. Ele também pode recusar um login que não iniciou.

Antes de confirmar ao NoPass a validade das credenciais, fatores adicionais podem ser executados, como verificar um token físico YubiKey ou uma prova biométrica. As opções dependem do dispositivo e dos recursos disponíveis. Por exemplo, iPhones e dispositivos Android possuem reconhecimento facial e impressões digitais.

Uma YubiKey também pode ser exigida para proteger uma máquina virtual ou estação compartilhada. Após a verificação local de segurança, o aplicativo envia

as credenciais ao servidor NoPass. Se forem válidas, o NoPass instrui o servidor de terceiros ou portal web a permitir o acesso do usuário ao aplicativo.

## Full Duplex Authentication® previne ciberataques comuns

A maioria dos ciberataques envolve roubo de credenciais. As organizações avançaram em ferramentas que impedem o uso de malware sofisticado e vulnerabilidades conhecidas. Por isso, invasores recorreram a ferramentas e métodos menos sofisticados, visando o elo mais fraco da segurança: as pessoas.

Full Duplex Authentication® oferece proteção adicional contra engenharia social porque o serviço solicitante sempre precisa se autenticar perante o usuário. Estes são alguns ataques e a forma como Full Duplex Authentication® os combate.

- Prevenção de phishing: Full Duplex Authentication® introduz desafios dinâmicos e respostas em todo o processo. A interação em tempo real entre o usuário e o servidor reduz a eficácia do phishing: credenciais estáticas, como senhas e tokens, sozinhas não bastam para autenticação bem-sucedida.

- Mitigação de Browser-in-Browser: a comunicação bidirecional do Full Duplex Authentication® permite verificar constantemente a legitimidade do navegador. Tentativas de injeção de código ou manipulação não autorizada são detectadas rapidamente, impedindo ataques de navegador dentro do navegador.
- Resistência a proxies maliciosos: Full Duplex Authentication® verifica constantemente a autenticidade e a origem do canal de comunicação. Essa resistência frustra as táticas dos proxies maliciosos e impede a interceptação e manipulação não autorizadas de dados.

## Impacto nos negócios

Como aponta o Verizon DBIR 2023, a maioria das violações de dados ocorre por meio de pessoas, o elo mais fraco da cadeia de segurança.

Além das possíveis perdas por acesso não autorizado, há custos operacionais associados à autenticação multifator baseada em senhas e

**Em 2023, o custo médio de uma violação de dados foi de US$ 4,5 milhões.**

Fonte: IBM

dispositivos físicos. Pelos riscos das senhas, elas precisam ser alteradas regularmente; a prática citada recomenda a cada 90 dias. Isso pode custar até uma hora de trabalho por senha por ano a uma organização.

Se dispositivos MFA forem perdidos ou apresentarem defeitos, sua substituição aumenta os custos operacionais. Os aplicativos Full Duplex Authentication® podem ser instalados em dispositivos que o funcionário já possui. O aplicativo executa pelo menos dois fatores, reduzindo significativamente os custos associados a outras ferramentas MFA.

## Conclusão

Diante de ameaças em evolução, medidas inovadoras são essenciais. Full Duplex Authentication®, descrita na patente dos EUA 11,245,526, está na vanguarda da autenticação moderna e oferece defesa dinâmica e robusta contra phishing, Browser-in-Browser e proxies maliciosos.

Implementar essa tecnologia inovadora e premiada é fundamental para proteger a integridade e a confidencialidade das interações on-line em um ambiente digital em transformação.

Full Duplex Authentication® permite eliminar senhas do fluxo de autenticação. Isso simplifica o processo e reduz os custos operacionais de gestão de senhas.

> Visite o site da Identité para conhecer nossas soluções MFA. Siga-nos no LinkedIn para receber notícias sobre segurança e gestão de identidades. Entre em contato com Vendas e solicite demonstrações.