UNICO

Segurança e privacidade de dados no Brasil

CENÁRIO ATUAL E PERSPECTIVAS

Sumário

01

Sobre a Unico

SOBRE A UNICO

Fundada em 2007, a Unico é líder em soluções seguras e confiáveis para a validação da identidade real das pessoas.

Após quatro rodadas de investimentos, a Unico conta com SoftBank, General Atlantics e Goldman Sachs como investidores. Em 2021, tornou-se unicórnio, sendo avaliada em mais de USD 2,6 bilhões.

Presente em mais de 800 empresas brasileiras, entre os maiores bancos privados, varejistas, fintechs, e-commerces e indústrias, a Unico dispõe de uma plataforma completa de capacidades inovadoras para a verificação e proteção da identidade. Essas capacidades incluem biometria facial para autenticação de identidades com 100% de certeza, camadas reforçadas de segurança para prova de vida, verificação de identidade e titularidade do cartão de crédito em compras online, admissão digital, gestão de compra de veículos e plataforma de educação corporativa.

Também foi reconhecida como uma das empresas mais inovadoras da América Latina pela Fast Company em 2024.

02

Segurança e privacidade

SEGURANÇA E PRIVACIDADE

O Brasil é destaque no cenário mundial de govtechs. Nos últimos anos, estes são alguns reconhecimentos recebidos pelo nosso país no que diz respeito ao desenvolvimento de soluções tecnológicas para o setor público:

2° país do mundo com a mais alta maturidade em governo digital, segundo o GovTech Maturity Index (GTMI) de 2022, feito pelo Banco Mundial

4° país da América do Sul com melhor oferta de serviços públicos digitais, de acordo com a pesquisa de 2022 das Organização das Nações Unidas (ONU)

Desempenho acima da média no Índice de Governo Digital de 2023, da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE)

Considerado pela 1ª vez como a economia mais inovadora da América Latina e Caribe, segundo o Índice Global de Inovação 2023, da Organização Mundial de Propriedade Intelectual

Para além do prestígio que esses títulos trazem para o Brasil, existe um aspecto prático na vida de quem reside no país: a facilidade de realizar transações do dia a dia ou de acessar serviços públicos e privados à distância.

SEGURANÇA E PRIVACIDADE

“Isso tem acrescentado uma eficiência muito importante, especialmente para as pessoas em situação de vulnerabilidade.”

Yasodara Cordova, pesquisadora-chefe de Privacidade de Dados na Unico

Mesmo com os avanços observados por aqui nos últimos tempos e com o prestígio internacional conquistado pelo Brasil nesse campo, a verdade é que ainda existem gargalos importantes a serem superados. Um deles foi objeto de estudo de uma pesquisa exclusiva da Unico encomendada à Fundação Getúlio Vargas (FGV), em 2022, que calculou o **Custo Brasil de Identificação (CBI)** - e seu impacto no Produto Interno Bruto (PIB).

O Brasil desperdiçou entre R$ 104 e R$ 175 bilhões de reais, ano, por usar processos analógicos de identificação.

SEGURANÇA E PRIVACIDADE

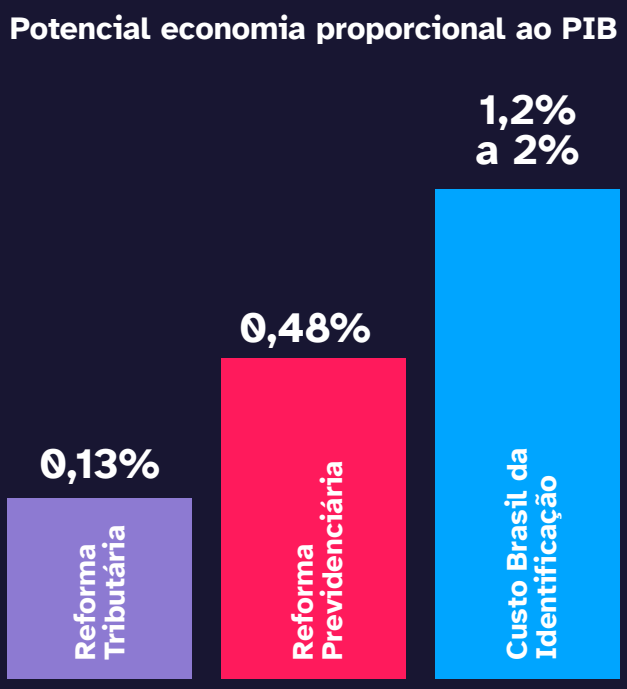
A Unico e a FGV fizeram uma comparação entre as perdas geradas pela ineficiência em processos de identificação e a economia esperada com reformas importantes, como a reforma da previdência e tributária. O resultado pode ser observado no gráfico abaixo:

O país perde 3x mais com a ineficiência em processos de identificação do que a economia esperada com reformas importantes.

A **Reforma Previdenciária** de 2019 deve representar redução de despesas em torno de 4,3% do PIB até 2060, resultado de um fluxo anual de cerca de 0,13%, de acordo com o Instituto Fiscal INdependente (IFI).

A **Refora Tributária** poderia representar um crescimento adicional do PIB brasileiro na casa de 5,42% até 2033, ou um fluxo próximo de 0,48% ao ano, segundo o Instituto de Pesquisa Econômica Aplicada (IPEA).

O **Custo Brasil da Identificação**, de ao menos 1,2% do PIB, é expressivo quando comparado ao impacto esperado de reformas como a tributária e previdenciária.



SEGURANÇA E PRIVACIDADE

No âmbito individual, nosso estudo mostrou que **o brasileiro perdeu um valor entre R$ 497,00 e R$ 830,00 no ano** para se identificar, o que representa de 41% a 68% do salário-mínimo da época (R$ 1.212,00). O cálculo foi baseado no gasto correspondente às atividades que exigem identificação física, como ter que ir presencialmente apresentar documentos ou assinar papéis.

O resumo da ópera é que a identidade digital se mostra como uma grande oportunidade para:

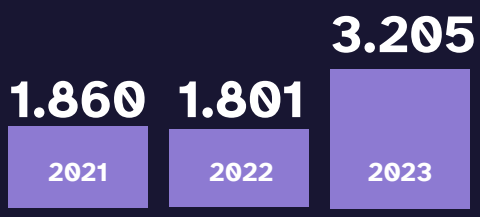
- **Automatizar** processos para **economizar recursos;**
- **Aumentar a conveniência** e a eficiência econômica;
- **Fornecer novas plataformas** para modernizar a prestação de serviços;
- **Projetar intencionalmente sistemas de identificação** para que sejam mais inclusivos e intuitivos;
- **Conferir maior autonomia às pessoas no que diz respeito à supervisão sobre como** os seus dados estão sendo utilizados.

SEGURANÇA E PRIVACIDADE

Apesar de todos os benefícios, é preciso ter em conta que esse processo tem seu lado B, **pois ao intensificar a digitalização, há também um aumento do risco de vazamento de dados.**

De acordo com o Relatório Anual de Violação de Dados de 2023, da Identity Theft Resource Center (ITRC), o número de dados comprometidos em 2023 aumentou 78% em comparação com 2022. Isso significou um novo recorde para a quantidade de dados comprometidos rastreados em um único ano, com um aumento de 72% em relação ao recorde anterior, que foi em 2021.

DADOS COMPROMETIDOS POR ANO

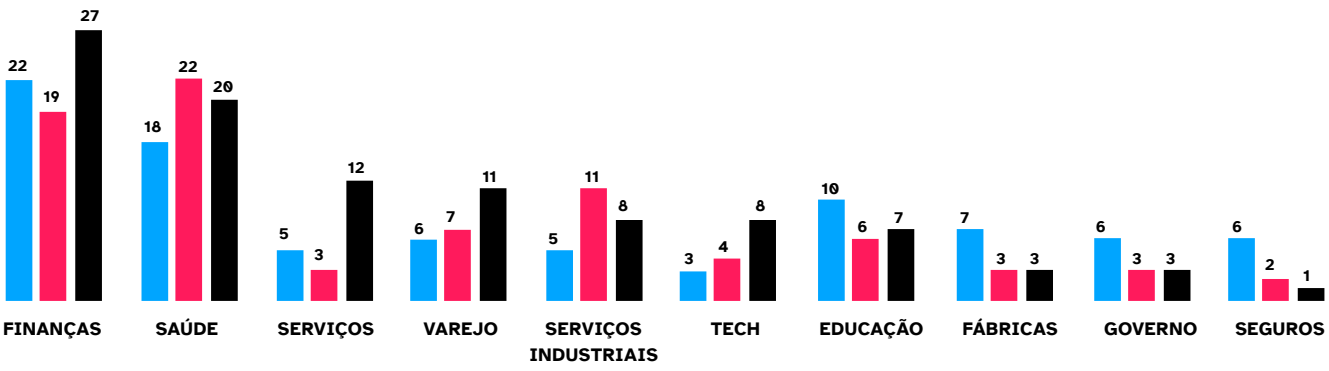


Fonte: Identity Theft Resource Center, 2023

A título de curiosidade, vale mencionar que, considerando o vazamento de dados, no período entre 2021 e 2023, os três setores com maiores incidências são financeiro, saúde e serviços.

Diante desse cenário, estamos, enquanto sociedade, diante de um paradoxo: se, de um lado, a digitalização traz benefícios, do outro ela representa ameaças. Como podemos, então, superar esse dilema?

% DE DADOS COMPROMETIDOS GLOBALMENTE, ENTRE 2021-23, POR INDÚSTRIA



FONTE: 2024 Data Breach Outlook, da Kroll

SEGURANÇA E PRIVACIDADE

“É importante termos em mente que, quando os países buscam adicionar eficiência à economia digitalizando os dados da população, é para a promoção de inclusão, acesso às oportunidades e melhorias nos processos de distribuição de benefícios e crescimento econômico. Ou seja, a digitalização é boa para nós, é boa para o mundo, mas sem mecanismos de proteção nos transformamos em alvos fáceis.”

Yasodara Cordova, pesquisadora-chefe de Privacidade de Dados na Unico

SEGURANÇA E PRIVACIDADE

Os pilares da proteção de dados

Apesar de não ser possível fugir desse paradoxo, podemos, sim, mitigar seu efeito por meio da privacidade, da segurança e da educação. Na Unico, acreditamos que o caminho passa por investir em uma identidade digital segura, apostar em um ecossistema confiável e conscientizar as pessoas para que elas possam zelar por sua segurança.

Refletir sobre esse tema complexo e, principalmente, adotar boas práticas para evitar danos ligados ao vazamento de dados é essencial para promover o funcionamento da democracia. Quando há clareza e transparência para todas as partes, os poderes permanecem em equilíbrio.

Isso significa que não só os governos e os cidadãos precisam estar atentos à pauta: esta é uma obrigação também das organizações corporativas. Todas as empresas precisam refletir sobre isso e, mais ainda, serem responsabilizadas.

Boa práticas para as companhias presentes no Brasil:

1. Não armazenar dados sensíveis em texto puro
2. Garantir integridade dos dados, sempre atualizados e sem modificações
3. Proteger senhas com funções de hash como bcrypt ou Argon2
4. Implementar autenticação multifator (MFA) para proteção de usuários
5. Manter controle interno de acessos com guarda de logs
6. Aplicar técnicas de pseudonimização ou anonimização
7. Considerar auditoria, mantendo gravações de acessos e modificação dos dados
8. Automatizar exclusão de dados que passam do prazo de retenção

03

Um panorama dos riscos e fraudes no Brasil

UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

Segundo a Federação Brasileira de Bancos (Febraban), os golpes mais aplicados no Brasil com uso de celular são:

- **GOLPE DO 0800 OU DA FALSA URA**
- **GOLPE DA TAREFA**
- **GOLPE DA CLONAGEM DO WHATSAPP**
- **ENGENHARIA SOCIAL COM WHATSAPP**
- ***PHISHING***
- **GOLPE DO ACESSO REMOTO**

Na próxima página, explicaremos do que se trata cada um deles, mas essas e outras “armadilhas” têm feito muitas vítimas no país.

Principais golpes aplicados com o uso do celular

GOLPE DO 0800 OU DA FALSA URA

O golpista envia mensagem para a vítima informando uma transação suspeita e solicitando que a pessoa entre em contato com a central de atendimento. No texto da mensagem, aparece um número 0800, que seria de uma central telefônica de um banco ou de uma área de cartões de crédito. Também são realizadas ligações telefônicas com uma gravação que simula as Unidades de Resposta Audível (URAs) das instituições financeiras.

Ao falar com a falsa central, a vítima é informada que a transação está em análise, por isso, ela ainda não aparece na fatura. Para cancelar a falsa operação, o golpista induz a pessoa a fazer uma transação ou fornecer dados pessoais, como número de conta e senha.

COMO EVITAR

Nunca faça ligações para números 0800 recebidos por mensagens. Se tiver alguma dúvida, ligue para os canais oficiais de seu banco ou para seu gerente.

GOLPE DA TAREFA

O criminoso manda uma mensagem se passando por um funcionário de uma empresa que está selecionando interessados para trabalhar de maneira online. A ideia é oferecer às vítimas uma oportunidade para ganhar dinheiro rápido e fácil em troca da realização de tarefas simples na internet, como curtir fotos, fazer comentários e seguir perfis de empresas e lojistas nas redes sociais.

Ao aceitar a proposta, a vítima é incluída em um grupo de mensagens. No começo, o golpista até deposita dinheiro para gerar credibilidade, mas sempre em valores baixos. Depois, ele explica que é necessário pagar para participar de outras tarefas, alegando que o participante recuperará o dinheiro no mesmo dia — e, assim, o golpe é aplicado.

COMO EVITAR

Sempre desconfie de propostas de trabalho que demandam pagamentos para garantir a vaga ou que prometem vantagens exageradas.

UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

GOLPE DA CLONAGEM NO WHATSAPP

O criminoso manda mensagens fingindo ser de uma empresa na qual a vítima tem cadastro. Ele solicita o código de segurança enviado por SMS, afirmando se tratar de uma atualização ou confirmação de cadastro. Assim, ele replica a conta de WhatsApp em outro celular e envia mensagens para os contatos da pessoa, se passando por ela.

COMO EVITAR

Uma medida simples é habilitar a opção de verificação em duas etapas no próprio aplicativo. Além disso, nunca informe o código de segurança do seu WhatsApp.

GOLPE DE ENGENHARIA SOCIAL COM WHATSAPP

O criminoso seleciona uma foto da vítima nas redes sociais, descobre os contatos da pessoa e manda mensagem para amigos e familiares da vítima, alegando que teve de trocar o número de celular devido algum problema. Então, ele pede uma transferência, dizendo estar em alguma situação de emergência.

COMO EVITAR

Ao receber uma mensagem de uma suposta pessoa conhecida, mas com um número novo, verifique se ela realmente mudou de telefone. Não faça qualquer tipo de transação até falar por outro meio com a pessoa que está solicitando o dinheiro, como uma ligação de vídeo, por exemplo.

UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

GOLPE DO *PHISHING*

O objetivo é conseguir senhas e dados pessoais do usuário. Geralmente, o golpe acontece por e-mail, simulando, por exemplo, a mensagem do seu banco. Nesse caso, o suposto banco afirma que a conta do cliente está irregular, que o cartão ultrapassou o limite ou que é necessário instalar um novo software de segurança.

Há também os casos em aplicativos de mensagens e nas redes sociais, levando o usuário a clicar em links maliciosos e em páginas falsas que solicitam senhas e/ou dados pessoais.

COMO EVITAR

Ao acessar um site, sempre verifique na barra do navegador se o endereço da página está correto. Não clique em links ou anexos de e-mails de remetentes desconhecidos. Para garantir, digite o endereço oficial da página que deseja acessar direto no navegador.

GOLPE DO ACESSO REMOTO

O fraudador entra em contato se passando por um falso funcionário do banco e usa várias abordagens para enganar o cliente, enviando um link para a instalação de um aplicativo que irá solucionar o suposto problema. O aplicativo é um malware que dá acesso ao celular.

COMO EVITAR

Os bancos nunca solicitam a instalação de aplicativo em seu celular para supostas regularizações na conta.

Todo esse cenário ganha novos contornos quando considerado o avanço da tecnologia que, por um lado, oferece recursos para lidar com as fraudes, mas, por outro, também se mostra como uma ferramenta nas mãos de criminosos. Um exemplo disso é o aumento do já citado golpe de *phishing* por conta da inteligência artificial (IA).

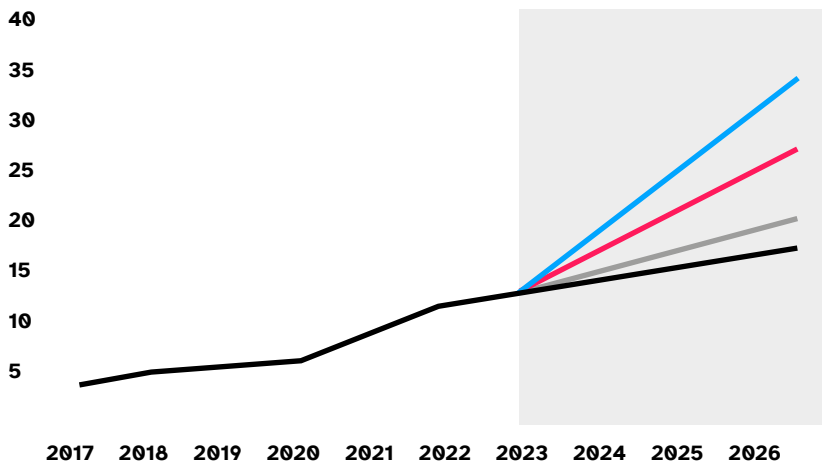
UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

Segundo o "Panorama de Ameaças de 2023", da Kaspersky, ferramentas que usam machine learning têm sido empregadas na criação de mensagens falsas. O resultado? As tentativas de golpes de *phishing* tiveram um aumento de 617% em comparação com os 12 meses anteriores.

A criação de mensagens de *phishing* cresceu 5x no Brasil

FONTE: Panorama de Ameaças de 2023, da Kaspersky

Esse fenômeno não é exclusivo do Brasil, é claro. De acordo com uma previsão do Centro de Serviços Financeiros da consultoria Deloitte, a IA generativa pode levar as perdas por fraudes nos Estados Unidos a atingirem US$ 40 bilhões até 2027, partindo de US$ 12,3 bilhões, em 2023 — o que representa uma taxa de crescimento anual composta de 32%.



PERDAS POR FRAUDE, REAIS E PREVISTAS, DE 2017 A 2027

(em bilhões de dólares americanos)

- Sem IA generativa
- Conservador
- Cenário base
- Agressivo

Fonte: 2024 Data Breach Outlook, da Kroll

Outro exemplo da utilização de IA em golpes tem a ver com uma palavra que ganhou os noticiários nos últimos tempos: ***deep fake***.

Confira o verbete no nosso glossário

Desde pessoas famosas, como o médico Drauzio Varella e o jornalista William Bonner, até civis comuns, esse recurso que pode criar áudios e vídeos digitalmente simulando a voz e/ou a aparência física de alguém tem usado a imagem de pessoas diversas para, além de aplicar golpes, disseminar desinformação e comprometer a reputação dos envolvidos.

UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

“É verdade que existe *deep fake* mal feito, mas tem aqueles muito bem feitos, que eu chamo de ‘*deep fake* de Hollywood’. E, veja, alguém com habilidade consegue produzir um material falso desse com 5 dólares ou menos. Por isso, precisamos tomar cuidado e não só pela nossa segurança, mas por aquela das pessoas ao redor. Cuidar dos nossos filhos, parentes, amigos para que eles não sejam vítimas nem do golpe, nem de ter sua imagem ou voz usada para manipular outras pessoas.”

Guilherme Bacellar, especialista e pesquisador de Cibersegurança e Fraudes da Unico

UM PANORAMA DOS RISCOS E FRAUDES NO BRASIL

Diante dessa realidade, é necessário rever nossas práticas e refletir se, de fato, estamos cuidando dos nossos dados como deveríamos. Afinal, maus hábitos podem levar a uma série de consequências não só no nível individual, mas coletivo, impactando inclusive a economia de um país.

Sobre os comportamentos danosos, vale destacar que, de acordo com um estudo encomendado pela Forbes Advisor, as pessoas cadastram a mesma senha em pelo menos quatro contas, em média. Não à toa, esse relatório indicou que **46% dos entrevistados tiveram suas senhas roubadas no último ano.**

Para não integrar essas e outras estatísticas assombrosas, a recomendação é fugir de péssimos hábitos como:

- ✕ **Utilizar senhas simples;**
- ✕ **Instalar aplicativos** no celular por fora das lojas oficiais, especialmente aqueles que prometem ofertas imperdíveis ou vantagens incríveis;
- ✕ **Fazer login em contas sensíveis** a partir de dispositivos que não são pessoais ou que não estão devidamente protegidos;
- ✕ **Compartilhar informações pessoais** e/ou sensíveis em redes sociais, aplicativos e formulários online sem a real necessidade.

> **“Nós temos maus hábitos que deixam nossos dados vulneráveis, facilitando o acesso de golpistas as nossas contas, deixando o caminho livre para sofrermos a fraude...”**

Guilherme Bacellar, especialista e pesquisador de Cibersegurança e Fraudes da Unico

O problema da falta de segurança de dados não se resolve apenas com esforços individuais. É necessária uma mobilização das forças políticas e corporativas, como tem sido observado em uma pauta quente de 2024: **a regulamentação das casas de apostas online.**

04

Bets e o que está em jogo no Brasil

PESQUISA

“Segurança digital: um olhar sobre jovens brasileiros”

Em parceria com o Instituto Locomotiva, a Unico realizou uma pesquisa exclusiva sobre “Segurança digital: um olhar sobre jovens brasileiros”. Dentre outros assuntos, o estudo investigou a relação de crianças e adolescentes com o universo dos games, incluindo sites de apostas esportivas e de cassino online. E uma das constatações é que os jogos online fazem parte do dia a dia de muitas pessoas no Brasil — não só dos adultos, mas dos menores de idade.

78% dos pais

86% dos filhos

jogam ou acessam games na internet

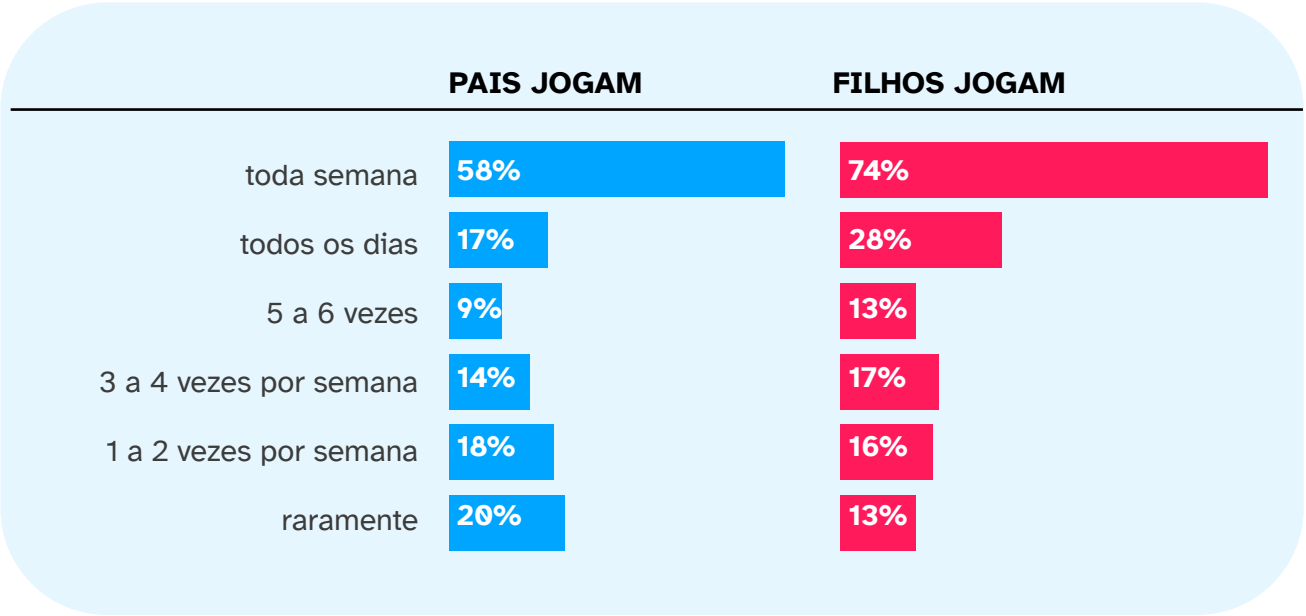
Metodologia

A pesquisa foi realizada em duas etapas: a primeira qualitativa, para consolidar o entendimento do problema da proteção de dados desse público no Brasil, e a percepção da vulnerabilidade de menores relacionadas à exposição de dados. Para isso, foram entrevistados com profundidade mais de nove especialistas na temártica.

Já a segunda etapa foi quantitativa, mensuramos as práticas e riscos online das famílias brasileiras a partir das declarações de pais e mães com filhos menores de idade. Com uma amostra nacional de 2.000 participantes, utilizamos pesquisa digital por autopreenchimento, realizada entre 9 e 24 de outubro de 2024. Os dados foram ponderados pela Pesquisa Nacional por Amostra de Domicílios (PNAD), do IBGE, considerando a população de 0 a 17 anos para a idade dos filhos e classe social, além da população a partir de 18 anos para a escolaridade dos pais.

BETS E O QUE ESTÁ EM JOGO NO BRASIL

Além da maior presença de crianças e adolescentes do que adultos no universo dos games, chama a atenção a frequência com que esse público mais novo fica em frente à tela — o que deve aumentar nas próximas semanas devido às férias escolares.



“Existem algumas razões para o aumento dessa frequência nas férias. Uma delas é que, com a proibição dos celulares nas escolas, aquele tempo em que crianças e adolescentes estavam fora das telas estará disponível de novo nas férias. Também tem a questão do Natal: outras pesquisas nossas identificaram ser cada vez mais comum presentear crianças e adolescentes com créditos de jogos. Então, nos próximos meses, essa utilização deve estourar”

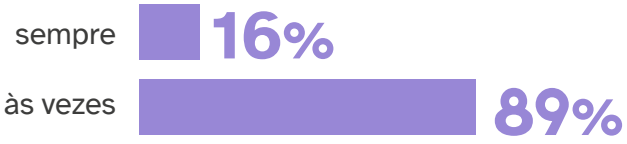
Renato Meirelles, presidente do Instituto Locomotiva

BETS E O QUE ESTÁ EM JOGO NO BRASIL

Para além da excessiva exposição às telas, essa forma de entretenimento — que, inclusive, pode ser positiva quando usada corretamente, por exemplo para fins educacionais — representa um grande risco à segurança de dados. Um risco que pode impactar os filhos e também os pais.

Isso porque, de acordo com o nosso levantamento, foi constatado que mais da metade das crianças e adolescentes que jogam online conversam ou interagem com desconhecidos (55%). Tal realidade se torna ainda mais preocupante quando analisada a frequência com que pessoas menores de idade interagem com outros jogadores que não conhecem, conforme é possível observar no gráfico abaixo.

Conversar/ interagir com outros jogadores que não conhece enquanto joga online



É nesse "solo fértil" que se dá a expansão das bets no Brasil. Segundo outro levantamento do Instituto Locomotiva, o número de brasileiros que apostaram nas bets nos últimos cinco anos chegou a 52 milhões. Desse total, 48% são considerados novos jogadores – ou seja, pessoas que apostaram nos primeiros sete meses de 2024.

Outro dado chocante, mas dessa vez da pesquisa do Locomotiva com a Unico, diz respeito a presença de pessoas entre 7 e 17 anos de idade nesse ambiente. De acordo com o estudo, 17% dos pais e mães declaram que o filho tem perfil em sites de apostas esportivas ou de cassino online. Acerca desse dado, é importante frisar que a porcentagem pode ser maior, já que o recorte é baseado naqueles que admitem que os filhos têm cadastro em tais lugares.

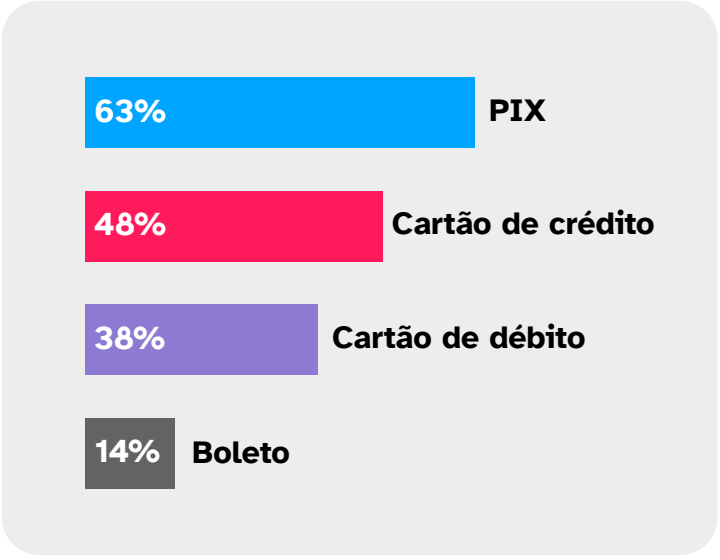
BETS E O QUE ESTÁ EM JOGO NO BRASIL

“Para mim, esse dado é alarmante porque estamos falando dos pais e mães que declararam que o filho tem perfil em sites de apostas esportivas ou de cassino online. Esses são os que sabem e admitem, mas e os outros? Os filhos podem estar nesse ambiente, mas os pais não sabem ou não querem admitir em uma pesquisa.”

Renato Meirelles, presidente do Instituto Locomotiva

O problema do desconhecimento se estende ainda para a questão do uso de formas de pagamento. Ao investigar os principais meios utilizados pelos filhos nas apostas online, a nossa pesquisa revelou que aproximadamente 13% dos pais simplesmente não sabem qual seria esse método. Dentre aqueles que souberam informar, as respostas apontaram, em sua maioria, para o PIX.

Tudo isso só reforça a urgência da regulamentação dos sites de apostas esportivas e de cassino online, que entra em vigor a partir de 1º de janeiro de 2025.



BETS E O QUE ESTÁ EM JOGO NO BRASIL

Contexto da regulamentação e os principais pontos em discussão

Em 2023, a Presidência da República enviou uma medida provisória ao Congresso Nacional para aprimorar a Lei 13.756/2018. Juntamente com outro projeto de lei que já estava em tramitação, a Câmara dos Deputados e o Senado Federal incluíram entre as apostas de quota fixa legalizadas no Brasil, os chamados jogos online. Foi, então, sancionada a Lei 14.790/2023, por meio da qual o Ministério da Fazenda recebeu a competência de regular o setor de apostas de quota fixa e criou, neste ano, a Secretaria de Prêmios e Apostas (SPA-MF).

“O que essa regulamentação fez foi, grosso modo, enxergar a pessoa que utiliza esse tipo de serviço de uma maneira muito próxima a de um consumidor, de modo a estabelecer direitos de consumidores para essa pessoa. Como esses direitos se dão? Justamente através da transparência de como funcionam esses algoritmos, quais são as reais chances de ganho em cassinos online etc.”

Felipe Magrim, diretor de Políticas Públicas e Relações Governamentais da Unico

BETS E O QUE ESTÁ EM JOGO NO BRASIL

No caso da proteção dos menores de idade, assunto urgente conforme demonstrado pela nossa pesquisa com o Instituto Locomotiva, isso é garantido por meio da obrigação das plataformas identificarem quem é o apostador. Funciona assim: no momento da abertura de uma conta, será solicitado o número de CPF desse usuário para uma consulta em uma base de dados a fim de entender se o documento é de um menor de idade ou não. A etapa seguinte de cadastro só será oferecida caso o documento pertença a uma pessoa maior de 18 anos.

Na sequência, entra a etapa de biometria facial — o que é diferente de reconhecimento facial e de prova de vida, conforme é possível verificar no nosso glossário. O objetivo, nesse momento, é verificar se a pessoa do outro lado da tela é, de fato, dona do CPF fornecido — processo que ocorre ao longo da jornada do consumidor.

Esse, aliás, é um diferencial importante dessa regulamentação: a garantia de que o processo de identificação aconteça durante a jornada completa do usuário e não somente no momento de abertura de uma conta.

Para isso, as portarias do Ministério da Fazenda estabeleceram em quais etapas deve se impor a obrigatoriedade da autenticação via biometria facial, para além do momento inicial da criação de uma conta. Alguns exemplos nesse sentido são:

Qualquer alteração do dado cadastral;

Reativação de conta;

Recuperação de uma senha;

Transações de cash out ou retirada de qualquer prêmio obtido na plataforma.

BETS E O QUE ESTÁ EM JOGO NO BRASIL

“O regulador optou por trazer essa questão da autenticação do jogador em vários momentos da experiência do usuário para ter certeza de que essa identificação está sendo feita o tempo inteiro. Através desse mecanismo, conseguimos trazer uma segurança maior, apesar de, é claro, nenhum instrumento ser 100%. Contudo, ainda assim, conseguimos ter mais segurança e mitigar a possibilidade de um menor de idade se expor ou expor os dados dos seus pais, um parente.”

Felipe Magrim, diretor de Políticas Públicas e Relações Governamentais da Unico

BETS E O QUE ESTÁ EM JOGO NO BRASIL

O que está sendo discutido e realizado coloca o Brasil como pioneiro no uso de biometria facial na regulamentação de jogos. Em comparação com o processo de outros países, os reguladores brasileiros foram muito mais rigorosos e cautelosos, porém, isso não significa que não devem surgir desafios pelo caminho.

“A Unico já está em ambiente de produção com alguns operadores brasileiros para que, no primeiro dia do ano, estejam prontos para o cumprimento da regulamentação.”

Felipe Magrim, diretor de Políticas Públicas e Relações Governamentais da Unico

Esse tipo de cuidado é fundamental para garantia não só da assertividade do processo, mas da reputação da tecnologia de biometria facial. Afinal, a falta de critérios de qualidade pode acabar prejudicando a percepção das pessoas sobre tecnologias de reconhecimento.

A oportunidade desse momento é mostrar, como aconteceu no setor financeiro, que inovação e regulamentação podem, sim, andar juntos. Contudo, para isso, é necessário operar uma transformação de forma criteriosa.

05

Bibliografia / Glossário

Fontes consultadas

This company is putting a face on fraud prevention for online purchases in Mexico and Brazil

2022 GovTech Maturity Index Update - GTMI

2023 OECD Digital Government Index

Índice Global de Inovação 2023: Suíça, Suécia e Estados Unidos lideram a classificação mundial de inovação; inovação mantém-se robusta, mas financiamento para startups é cada vez mais incerto.

Custo Brasil da Identificação - Unico.

Relatório de Fraude da Serasa Experian: 4 em cada 10 brasileiros já foram vítimas de golpes e preocupação de empresas aumentou 58% em um ano

Identity Theft Resource Center 2023 Annual Data Breach Report Reveals Record Number of Compromises; 72 Percent Increase Over Previous High

Inteligência Artificial, para o bem ou mal: relatório da Kaspersky mostra que ataques de phishing aumentaram com o uso da IA

Generative AI is expected to magnify the risk of deepfakes and other fraud in banking

America's Password Habits: 46% Report Having their Password Stolen Over the Last Year – Forbes Advisor

Bets: 86% das pessoas que apostam têm dívida e 64% estão negativadas na Serasa, diz pesquisa - Instituto Locomotiva

Regulamentação da legislação de bets torna atividade mais segura no Brasil

Mercado das apostas online precisa ser regulamentado para toda a população

Conheça os principais golpes aplicados com o uso do celular e saiba como evitá-los

Mais de 22 milhões de pessoas apostaram nas 'bets' no último mês, revela DataSenado

Glossário

171
Termo para determinar fraudes, fraudadores e todo o ecossistema de fraudes.

A

Anjo
Código de segurança (numérico de 6 dígitos) para acessar a conta bancária ou realizar uma operação. Também conhecido como OTP ou Token, podendo ser em formato de chaveiro ou gerado por aplicativo no celular.

Assinatura eletrônica
É uma forma de confirmar quem criou ou autorizou um documento eletrônico. Funciona como uma “assinatura virtual” que pode ser usada para identificar o autor de um arquivo digital.

Assinatura digital
É um tipo mais seguro de assinatura eletrônica. Nesse caso, é usada uma tecnologia especial que cria duas “chaves”: uma privada, que só o dono usa, e outra pública, que qualquer pessoa pode usar para conferir a validade da assinatura. Com isso, o dono pode assinar um documento digital usando sua chave privada para mostrar que concorda com o conteúdo. Quem recebe o documento usa a chave pública para verificar se a assinatura é verdadeira e se o documento não foi alterado depois de assinado.

Autenticador
Os autenticadores são ferramentas que oferecem uma camada extra de proteção aos clientes. Isso porque eles confirmam a identidade de um cliente durante o processo de login ou checkout em uma página de e-commerce e no momento do pagamento. Isso pode ser feito por meio de perguntas que somente a pessoa sabe a resposta ou por biometria. Embora esse sistema possa provocar atrito à experiência do cliente, evita que as contas dos usuários sejam comprometidas.

Ataque teardrop
Tipo de ataque de negação de serviço (DoS) que utiliza pacotes de dados fragmentados para sobrecarregar o servidor ou a rede de uma vítima. Como o servidor não consegue remontar os pacotes corretamente, isso provoca uma sobrecarga e, consequentemente, o desligamento do sistema. Ataques teardrop geralmente têm como alvo servidores que possuem vulnerabilidades existentes no protocolo TCP/IP. Esses ataques exploram o modo como os pacotes IP são fragmentados e remontados para evitar os controles de segurança tradicionais em servidores locais ou redes. São mais comuns em governos locais, hospitais e pequenos bancos, especialmente naqueles que utilizam sistemas operacionais muito antigos (como o Windows 95 ou anteriores).

AVS
O sistema de verificação de endereço (AVS) é um filtro de fraude que diversos comércios eletrônicos usam para bloquear pedidos potencialmente fraudulentos. Para a transação ser aprovada, as partes numéricas dos endereços de cobrança e remessa que um cliente insere devem corresponder às registradas no banco emissor do cartão. Caso contrário, a transação pode ser recusada ou sinalizada para revisão manual.

B

Bico
Denota principalmente um trabalho ou um golpe, mas também pode ser aplicado ao usuário alvo de fraude.

BIN
São os 6 (podendo em alguns casos serem os 8) primeiros dígitos do número do cartão de crédito.

Biometria facial
Tecnologia que realiza a medição e análise de características faciais únicas de um indivíduo, como distância entre os olhos e formato do nariz, que serve como uma forma de identificar especificamente cada pessoa e autenticar sua identidade. É considerada uma das tecnologias mais seguras do mundo, e é mais eficaz do que o reconhecimento facial que faz um *match* de foto com foto.

Botnet
Esse termo é uma combinação das palavras “robô” (bot) e “rede” (net). Em geral, se refere a uma sequência maliciosa de dispositivos conectados à internet, utilizados para roubar dados e comprometer outros computadores e sistemas.

Burlador
Software que visa enganar sistemas de prova de vida e biometria facial, permitindo a utilização de fotos externas em vez da captura legítima pela câmera.

C

Carder
Fraudador que opera cartões de crédito (seja obtendo, validando ou vendendo).

Catfishing
Golpes de Namoro Online
Catfishers criam identidades falsas em aplicativos de namoro e redes sociais para enganar pessoas em relacionamentos online fictícios. Frequentemente, eles rapidamente migram para canais pessoais, como telefone ou e-mail, usando sua confiança para obter dinheiro, informações pessoais ou até mesmo para ajudá-los a encobrir atividades criminosas. Provavelmente, você nunca os encontrará pessoalmente.

Checker
Aplicativos ou sites (painéis) que são utilizados para testar e validar se os dados que o fraudador possui são bons e estão funcionando/aptos a serem utilizados. Entre os dados estão informações de cartão de crédito, email + senha ou dados de acesso a contas bancárias.

Cramming
Cramming ocorre quando operadoras de telefone ou empresas de cobrança de terceiros adicionam cobranças enganosas, não autorizadas, fraudulentas ou mal explicadas na conta telefônica.

Criptografia de ponta a ponta (E2EE)
Método de comunicação seguro no qual os dados são criptografados no dispositivo de origem e só podem ser decifrados no dispositivo de destino. Durante o tráfego de dados entre os pontos, as informações permanecem cifradas, garantindo que terceiros, como provedores de serviço ou hackers, não possam acessar o conteúdo transmitido, mesmo que consigam interceptá-lo. Isso protege a privacidade e a integridade da comunicação.

D

Dark web
É uma parte oculta da internet que não é indexada por mecanismos de busca regulares, sendo acessada por meio de navegadores especializados como o Tor. Ela abriga tanto atividades legais quanto ilegais, oferecendo anonimato, mas também apresentando riscos, como golpes e conteúdo ilícito.

DB
Conjunto de muitos dados (por vezes uma grande quantia) podendo conter dados pessoais, informações de cartão de crédito ou de acesso a contas.

Deepfake
Tipo específico de mídia sintética em que a imagem ou vídeo de uma pessoa é substituída pela aparência de outra. O termo foi cunhado pela primeira vez no final de 2017 por um usuário do Reddit, que criou um espaço na plataforma onde compartilhava vídeos pornográficos que utilizavam tecnologia de troca de rosto de código aberto. Desde então, o termo se expandiu para incluir "aplicações de mídia sintética" que já existiam antes da página no Reddit, além de novas criações como o StyleGAN — imagens estáticas realistas de pessoas que não existem, segundo Henry Ajder, chefe de inteligência de ameaças da empresa de detecção de deepfakes Deeptrace.

Deep web
Refere-se ao que está abaixo da superfície e representa aproximadamente 90% de todos os sites. Essa seria a parte de um iceberg submersa na água, muito maior do que a web de superfície. Essa web oculta é tão extensa que é impossível determinar exatamente quantas páginas ou sites estão ativos em um dado momento. Seguindo a analogia, grandes mecanismos de busca podem ser considerados como barcos de pesca que só conseguem "capturar" sites próximos à superfície. Todo o restante, desde revistas acadêmicas até bancos de dados privados e conteúdos mais ilícitos, está fora de alcance. A deep web também inclui a porção que conhecemos como dark web. Embora muitos meios de comunicação usem os termos "deep web" e "dark web" de forma intercambiável, grande parte da porção profunda como um todo é perfeitamente legal e segura.

E

Editáveis
Modelos de documentos (RG, CNH, CPF, Comprovantes de Endereço, Carteira de Trabalho, etc) na qual o criminoso pode editar os campos e colocar a foto que deseja.

Esquemas
Macetes, dicas, segredinhos para o sucesso da execução da fraude. Exemplo: No banco Y utilize o navegador Firefox durante a madrugada que é certeza do sucesso.

F

Falsas recusas
As falsas recusas (ou falsos positivos, como também são chamadas) ocorrem quando uma transação legítima é sinalizada pelo sistema de proteção contra fraudes e recusada. Em geral, isso pode acontecer quando o titular do cartão solicita o envio dos produtos comprados para endereço diferente do cadastrado. Com isso, o cliente é identificado erroneamente como fraudador e não consegue finalizar a compra.

Filtros de velocidade
Os filtros de velocidade monitoram elementos de dados específicos (como endereço de e-mail, número de telefone e endereços de cobrança/envio). Eles limitam o número de transações que um site pode processar em um determina do período (uma hora, um dia). Isso evita que um fraudador tenha tempo para testar diversos números de cartões roubados, a fim de verificar se funcionam.

I

Identidade digital
No seu nível mais básico, método pelo qual cada pessoa se identifica perante um site na Web, ou num serviço da internet. Atualmente há muitas formas de o fazer, usando elementos como nomes do utilizador, palavras-passe, números de identificação pessoal (PINs) e certificados digitais.

Info Banker
Informações que permitem o acesso a contas bancárias. No geral é composto por CPF, senha ou agência e/ou conta + senha.

Informações de identificação pessoal ou *Personally identifiable information (PII)*
Toda informação relacionada a um indivíduo específico, que pode ser usada para descobrir sua identidade, como número de previdência social, nome completo, endereço de e-mail ou número de telefone. À medida que as pessoas passaram a confiar cada vez mais na tecnologia da informação tanto na vida pessoal quanto profissional, a quantidade de IIP compartilhada com as organizações aumentou.

L

Lara
Contas, sejam bancárias ou e-commerce, em nome de terceiros que são operadas pelos criminosos com o objetivo de realizar pagamentos, vendas, receber pagamentos ou centralizar fundos para transferência posterior.

Lotter
Define um caloteiro. Alguém que não cumpre o combinado ou ativamente está tentando passar golpe nos fraudadores.

M

Material
Todo e quaisquer tipos de produtos comercializados pelos fraudadores, como: Esquemas, modus-operandi, manuais, softwares, dados de terceiros etc.

P

Passwordless
Recurso para fortalecer a segurança e abolir o uso de senhas. Ele já é realidade em diversas empresas no Brasil e no mundo, de modo que a tendência é que todas as empresas contem com esse mecanismo para verificação de identidade. No lugar das senhas, um dos principais métodos de identificação utilizados é o da biometria. Dessa maneira, em vez de ser identificado com uma combinação alfanumérica, o usuário será reconhecido por meio de características únicas e específicas, como no caso da biometria facial, por exemplo.

Phishing
Golpistas frequentemente utilizam o “phishing” por e-mail para fisgar vítimas de fraude desavisadas. Considere todos os e-mails não solicitados e spam como suspeitos: não abra nem responda. Para evitar carregar softwares maliciosos em seu computador ou dispositivo, nunca clique em links — mesmo de uma fonte confiável — sem verificar sua autenticidade. Tenha cuidado especial com e-mails que pedem fundos de emergência ou ajuda de amigos, familiares e colegas. As contas de e-mail deles podem ter sido hackeadas. Golpistas também se passam por agências governamentais em e-mails fraudulentos.

Privacidade de dados
É o direito que as pessoas têm de proteger suas informações pessoais, garantindo que elas não sejam acessadas ou expostas sem sua permissão. Ou seja, é o direito ao controle de cada um sobre o que será compartilhado sobre sua vida íntima e privada.

Privacidade diferencial
Padrão para cálculos em dados que limita as informações pessoais reveladas por uma saída. A privacidade diferencial é normalmente usada para compartilhar dados e permitir inferências sobre grupos de pessoas, além de impedir que alguém aprenda informações sobre um indivíduo. A privacidade diferencial é útil quando há risco de reidentificação e para quantificar a compensação entre risco e utilidade analítica.

Privacy-enhancing technologies (PET) ou tecnologias de aprimoramento de privacidade
As tecnologias de aprimoramento da privacidade (Privacy Enhancing Technologies - PETs) permitem a coleta, análise e compartilhamento de informações enquanto protegem a confidencialidade e a privacidade dos dados. Elas complementam os frameworks de proteção de privacidade e confidencialidade, mas exigem orientações claras para enfrentar os desafios regulatórios e técnicos. Seu desenvolvimento, maturidade e integração eficaz também dependem de superar os desafios de adoção, além de reduzir lacunas de conhecimento.

Prova de vida ou liveness detection
Tecnologia responsável por dizer se a pessoa é real, se está em frente à câmera ao vivo no momento da captura da biometria facial. Essa tecnologia reconhece imagens e vídeos que foram manipulados para serem usados em fraudes, principalmente financeiras, ou ataques de apresentação, como máscaras.

PVC
Cartões de crédito ou débito em forma física.

Puxada
Ato de consultar os dados completos (Dados pessoais, bancários, endereços, telefones, email, parentes, empregos, renda, etc) de uma pessoal através de informações pessoais (CPF, Telefone, Email), podendo ser realizado em sites disponíveis pelos fraudadores (conhecidos como paineis) ou em grupos de conversa.

R

Reconhecimento facial
Tecnologia que verifica uma pessoa analisando e comparando características de imagens ou vídeos contra um banco de dados de fotos de faces já conhecidas, comumente utilizada em sistemas de segurança, desbloqueio de celular, catracas, acesso a prédios etc.

Referências
Evidências apresentadas por outras pessoas que já fizeram negócios com um vendedor e que provam a veracidade/funcionamento de algo sendo vendido, desta forma garantindo que o vendedor irá entregar corretamente o que está sendo negociado.

T

Tela Fake
Site falso que copia o mais fielmente possível um site legítimo de banco, comércio eletrônico, governo ou empresa de serviços. São criados para obter informações das vítimas, como: Dados pessoais, fotos de documentos, comprovantes de residência e fotos da face.

Tokenização
Os serviços de pagamento como Apple e Android utilizam a tokenização para proteger os dados confidenciais, trocando as informações pessoais por dados gerados aleatoriamente. Dessa forma, os dados reais do cartão de crédito de uma pessoa nunca são acessados ou usados. Esse é um processo sem atrito e quase invisível para os consumidores. Além disso, ajuda a proteger contra o roubo de dados do cartão de crédito durante uma transação e auxilia os comerciantes a cumprir os padrões de segurança do setor, como o PCI DSS.

Trampos ON / Trampos OFF
Denota um esquema fraudulento que está funcionando (Trampos ON) ou não está mais funcionando (Trampos OFF). Também pode denotar que um fraudador em específico está trabalhando em um esquema bom (Trampos ON) ou está em ausência por quaisquer motivos (Trampos OFF).

V

Verificação de identidade

W

Web scraping ou “raspagem de dados”
Colheita ou extração de dados na web, refere-se basicamente à coleta de dados de sites por meio do Protocolo de Transferência de Hipertexto (HTTP) ou por meio de navegadores da web.

Contato

Ficou com alguma dúvida ou gostaria de entrevistar um dos nossos porta-vozes?

É só mandar um e-mail para unico@beet.house
ou falar diretamente com o Renan (11 99136-3355) ou a Cata (11 99355-3346).