PROTEÇÃO FINANCEIRA PARA EMPREENDEDORES

ESTRATÉGIAS PARA MITIGAR RISCOS CIBERNÉTICOS, PREVENIR FRAUDES E PROMOVER A SEGURANÇA DA INFORMAÇÃO

SEBRAE

PRESIDENTE DO CONSELHO DELIBERATIVO ESTADUAL
Robson Carneiro

DIRETOR-SUPERINTENDENTE
Antonio Alvarenga Neto

DIRETOR DE DESENVOLVIMENTO
Sergio Malta

DIRETOR DE PRODUTO E ATENDIMENTO
Júlio Cezar Rezende de Freitas

GERÊNCIA DE INOVAÇÃO E SOLUÇÕES
Raquel Abrantes de Figueiredo Silva – Gerente

COORDENAÇÃO DE CAPITALIZAÇÃO E SERVIÇOS FINANCEIROS
Marcos Antonio de Souza Mendes – Coordenador
Maria Cláudia Salles Vianna – Analista

GERÊNCIA DE EDUCAÇÃO
Antônio Carlos Kronemberger – Gerente

COORDENAÇÃO DE EDUCAÇÃO EMPREENDEDORA
Amanda Alexandre Borges Fernandes – Coordenadora
Renata Mauricio Macedo Cabral – Analista
Milton Ferreira Dias Júnior – Design Gráfico

CONSULTORIA
Rosana Santos – Conteudista
Faros Educacional – Revisão gramatical e ortográfica

Bibliotecário catalogador – Leandro Pacheco de Melo – CRB 7ª 5471

S237 Santos, Rosana.
Proteção financeira para empreendedores : estratégias para mitigar riscos cibernéticos, prevenir fraudes e promover a segurança da informação / Rosana Santos. – Rio de Janeiro: Sebrae/RJ, 2024.
23 p.

ISBN 978-65-5818-545-1

1. Finanças. 2. Proteção financeira. 3. Cibersegurança. I. Sebrae/RJ. II. Título.

CDD 658.15
CDU 004.056.5:658.15

Súmario

Introdução 4

Conscientização sobre ameaças cibernéticas 5

Identificação de sinais de alerta 9

Práticas de segurança cibernética/Recursos de segurança da informação 9

Uso seguro de dispositivos eletrônicos/Segurança de dispositivos eletrônicos 10

Ferramentas de proteção cibernética 11

Seguros 12

Combater e prevenir fraudes 13

Tipos Comuns de Fraudes Financeiras / Conscientização sobre Golpes e Esquemas Fraudulentos 13

Prática de prevenção de fraudes 14

Uso seguro de cartões de crédito, débito e PIX 15

Educação sobre engenharia social 17

Promover a segurança da informação: 21

Conscientização sobre a importância da segurança da informação 21

Práticas de segurança de dados pessoais/Gestão de senhas e credenciais de acesso 21

Segurança de redes Wi-Fi e conexões on-line 23

Proteção contra roubos de identidade 24

Leitura crítica 25

Encerramento 26

Introdução

Com o avanço da tecnologia, os golpes financeiros evoluem constantemente, demandando uma atenção redobrada dos empreendedores. A comodidade de realizar transações bancárias, vendas, compras e investimentos de forma rápida e acessível através de dispositivos – como celular e notebook – é uma “mão na roda”. No entanto, essa praticidade vem acompanhada de uma série de desafios e precauções que você precisa ter em mente.

Segundo dados de uma pesquisa publicada em 2023, realizada pela Confederação Nacional de Dirigentes Lojistas (CNDL) e pelo Serviço de Proteção ao Crédito (SPC Brasil) em colaboração com o Sebrae, cerca de 22% dos entrevistados reportaram terem sido vítimas de algum tipo de fraude em instituições financeiras nos últimos 12 meses. Isso equivale a aproximadamente 8,4 milhões de consumidores afetados por práticas fraudulentas.

Diante desse cenário preocupante, é fundamental que empreendedores estejam devidamente preparados para mitigar riscos financeiros cibernéticos, combater e prevenir fraudes, além de promover a segurança da informação em seus negócios. Este e-book foi elaborado com o intuito de fornecer as ferramentas e estratégias necessárias para que você possa proteger a si mesmo e o seu empreendimento contra ameaças financeiras.

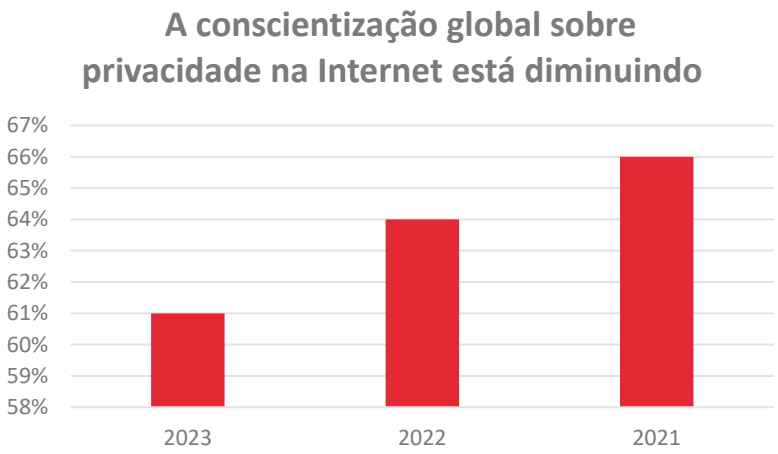
Ao longo deste material, você encontrará orientações práticas, dicas valiosas e melhores práticas recomendadas por especialistas, desde os principais tipos de golpes e fraudes mais comuns até as medidas preventivas que podem ser adotadas para proteger as finanças do seu negócio e dos seus clientes.

Prepare-se para aprofundar seus conhecimentos, fortalecer a segurança do seu empreendimento e garantir a tranquilidade necessária para focar em seu crescimento e sucesso.

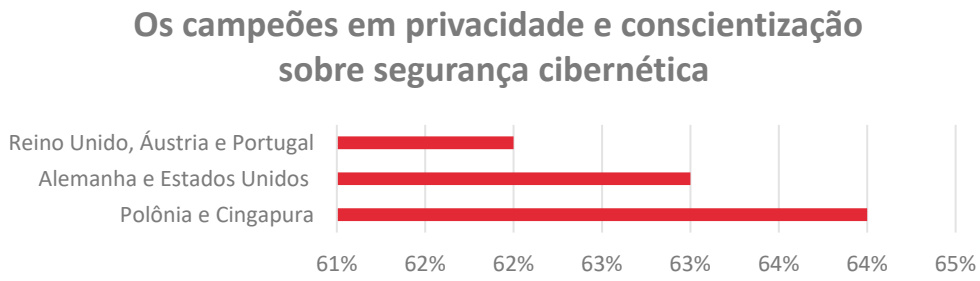
Conscientização sobre ameaças cibernéticas

GRÁFICOS

Evolução do Brasil em cibersegurança



A pontuação global do NPT[1] atingiu (61%) este ano, o que mostra diminuição da privacidade on-line e da conscientização sobre segurança cibernética do mundo em comparação com 2022 (64%) e 2021 (66%). Muitos ainda subestimam a importância de ler os termos de serviço. No entanto, essa métrica está melhorando mais rapidamente do que outras. As pessoas com idade entre 30 e 54 anos, por exemplo, têm as melhores habilidades de segurança cibernética, em comparação com outras faixas etárias.



1. Polônia e Cingapura (64%)
2. Alemanha e Estados Unidos (63%)
3. Reino Unido, Áustria e Portugal (62%)

[1] O National Privacy Test (NPT) é um estudo mundial, anual e de acesso aberto que qualquer pessoa pode responder. Destina-se a avaliar a segurança cibernética e a conscientização sobre privacidade on-line. Vale ressaltar que a pesquisa não definiu cotas de idade e sexo. O relatório compara dois conjuntos de dados: um foi coletado durante um período de seis meses em 2023, enquanto o outro cobre o ano de 2021.

https://securityleaders.com.br/brasileiro-e-o-5o-no-mundo-em-conhecimento-de-ciberseguranca-mas-protecao-de-dados-e-desafio/

É essencial conscientizar os microempreendedores sobre as ameaças cibernéticas, como *phishing*, malware e ataques de engenharia social (os tipos mais comuns enfrentados pelos consumidores financeiros), que podem causar danos significativos aos seus negócios. O *phishing* pode resultar em vazamento de dados de clientes, comprometendo a confiança e a reputação da empresa, enquanto o malware pode causar interrupções nas operações e perda de dados críticos. Além disso, os ataques de engenharia social podem levar à divulgação de informações sensíveis, comprometendo a segurança geral do negócio. Portanto, é crucial implementar medidas de segurança robustas e oferecer treinamento regular aos funcionários para mitigar essas ameaças e proteger a integridade do empreendimento. Vamos verificar como essas ameaças podem afetar as finanças pessoais.

Phishing

O *phishing* é um tipo de ataque cibernético em que os criminosos tentam enganar as pessoas para obter informações pessoais, como senhas e detalhes de cartão de crédito, por meio de mensagens fraudulentas que parecem legítimas.

Os ataques de *phishing* podem provocar sérios danos à vida financeira das pessoas. Veja as principais táticas utilizadas pelos criminosos a seguir:

Roubo de informações financeiras:

- Golpistas solicitam dados financeiros, como números de cartão de crédito ou dados de login de contas bancárias;
- Usam pretextos como atualizações de segurança ou promoções falsas. Uma vez obtidas, as informações permitem acesso às contas das vítimas para transações não autorizadas.

Fraudes de transferência de dinheiro:

- Golpistas pedem que as vítimas realizem transferências para contas falsas;
- São apresentadas histórias convincentes, como pedidos de ajuda em emergências ou ofertas de negócios lucrativos;
- As vítimas podem enviar dinheiro sem perceber que estão sendo enganadas.

O *phishing* pode acontecer de diversas maneiras, entre elas por SMS ou por ligação telefônica (e mais recentemente por IA – Inteligência Artificial [veja sobre isso mais a frente]).

Malware

Worms, ou "vermes de computador", se diferenciam de outros tipos de software malicioso por sua capacidade única de se replicar automaticamente e se propagar por redes sem a necessidade de intervenção humana.

Ransomware é um tipo de malware que criptografa os arquivos do computador da vítima e exige um resgate (ou "ransom") para desbloquear o acesso aos dados.

O malware, ou software malicioso, é um programa desenvolvido para danificar dispositivos e redes. Ele inclui várias formas, como vírus, *worms* e *ransomware*, representando uma ameaça à segurança financeira e podendo levar ao roubo de informações e acesso não autorizado a contas bancárias. Para se proteger, é crucial usar software de segurança atualizado e estar ciente dos riscos on-line.

O malware pode ameaçar a segurança financeira das pessoas de várias maneiras:

Instalação de malware financeiro:

- Golpistas induzem vítimas a clicarem em links ou baixarem arquivos maliciosos;
- Os arquivos baixados infectam dispositivos;
- Informações financeiras armazenadas são roubadas, como dados de login bancário.

Roubo de informações financeiras:

- Roubo de números de cartão de crédito, dados bancários e senhas;
- São realizadas transações não autorizadas ou roubo de identidade.

Acesso não autorizado a contas bancárias:

- Acesso não autorizado às contas bancárias das vítimas;
- Criminosos podem realizar transferências de dinheiro sem consentimento.

Ransomware:

- Arquivos do computador são criptografados e exige-se resgate para desbloqueio;
- Sem o pagamento, vítimas podem perder acesso a documentos financeiros importantes.

Manipulação de transações financeiras:

- Interferência em transações financeiras, alterando detalhes de pagamento;

- Redirecionamento de fundos para contas controladas por criminosos.

Engenharia social

Worms, ou "vermes de computador", se diferenciam de outros tipos de software malicioso por sua capacidade única de se replicar automaticamente e se propagar por redes sem a necessidade de intervenção humana.

Ransomware é um tipo de malware que criptografa os arquivos do computador da vítima e exige um resgate (ou "ransom") para desbloquear o acesso aos dados.

Autenticação em dois fatores é um método de segurança que exige duas etapas de verificação para acessar uma conta, tornando-a mais segura contra hackers. Exemplo de autenticação em duas etapas: digitar sua senha e um código enviado para seu celular.

QUADRO

(Imagem referência)

Título: Engenharia social: como fraudadores manipulam suas vítimas – 4 passos para realizar uma fraude através da engenharia social

Coleta de informações: o fraudador reúne detalhes sobre a vítima, como informações pessoais e hábitos, geralmente através de pesquisa on-line ou contato direto.

Estabelecimento de confiança: após coletar informações, o fraudador procura construir uma relação de confiança com a vítima, frequentemente se passando por alguém conhecido, uma autoridade ou um prestador de serviços confiável.

Manipulação emocional: uma vez estabelecida a confiança, o fraudador utiliza táticas emocionais para manipular a vítima, explorando sentimentos como compaixão, urgência, medo ou gratidão para induzi-la a agir conforme seus interesses.

Solicitação de ação: na etapa final, o fraudador solicita à vítima que realize uma ação específica, como fornecer informações confidenciais, clicar em links maliciosos, efetuar um pagamento ou executar outra medida que beneficie o fraudador.

Identificação de sinais de alerta

Estar vigilante e realizar monitoramento regular das transações pode ajudar a detectar atividades fraudulentas e proteger suas finanças on-line.

Por isso, mantenha-se atento a:

- Atividades não reconhecidas em extratos bancários;
- Aparição de contas ou cobranças desconhecidas;
- Solicitações de informações pessoais ou financeiras suspeitas, por e-mail ou telefone;
- Alterações repentinas nos padrões de gastos ou recebimentos;
- Acesso não autorizado a contas ou serviços on-line;
- Mensagens ou notificações suspeitas durante transações on-line;
- Erros inesperados ou problemas ao acessar contas financeiras;
- Histórico de pagamentos estranhos;
- E-mails ou mensagens de texto suspeitos com anexos ou links, que podem ser uma tentativa de *phishing* para roubar suas informações pessoais.

Práticas de segurança cibernética/Recursos de segurança da informação

Apresentamos diretrizes de segurança cibernética para proteger informações pessoais e financeiras on-line, incluindo precauções ao usar Wi-Fi público e métodos para detectar fraudes por e-mail ou sites. Essas orientações visam garantir a segurança dos usuários na internet:

Diretrizes de Segurança Online: Protegendo-se Contra Fraudes e Ataques Cibernéticos	
O QUE	**COMO SE PROTEGER**
Compartilhamento de informações pessoais	• Evitar fornecer informações sensíveis em conexões Wi-Fi públicas ou não confiáveis; • Nunca inserir informações pessoais ou financeiras em pop-ups suspeitos; • Não salvar o número do cartão de crédito em dispositivos ou navegadores.
Autenticidade	• Verificar a autenticidade dos sites visitados; • Procurar por certificados SSL (Secure Socket Layer) e ícone de cadeado na barra de endereços; • Analisar detalhes do certificado SSL e registro do domínio.
Atratividade exacerbada	• Desconfiar de ofertas e promoções muito tentadoras; • Atentar-se a *phishings*, pois podem usar ofertas atraentes para direcionar vítimas a sites falsos.
Antivírus	• Usar antivírus e softwares de proteção; • Utilizar extensões de navegador que detectam *phishing* e atividades suspeitas.
Medidas preventivas	• Utilizar cartões de crédito temporários ou métodos de pagamento que não permitam reutilização dos dados; • Cuidar da segurança das senhas com autenticação de dois fatores e gerenciadores de senhas.
Como identificar sites e e-mails fraudulentos:	• Verificar o endereço de e-mail, inspecionar os links e evitar abrir anexos de desconhecidos; • Conferir domínio, URL e selos de segurança dos sites; • Pesquisar pela reputação e histórico do site, além de confirmar as informações de contato antes de realizar compras.

Uso seguro de dispositivos eletrônicos/Segurança de dispositivos eletrônicos

O texto "**Segurança em dispositivos móveis – 10 passos para se proteger**" (https://eval.digital/seguranca-em-dispositivos-moveis-10-passos-para-se-proteger/), da Eval Digital, destaca a importância de proteger as informações pessoais e profissionais em dispositivos móveis e oferece 10 dicas simples e eficazes para evitar violações de privacidade e roubo de identidade, independentemente do grau de conhecimento em tecnologia. As medidas são essenciais para garantir a segurança digital em um mundo cada vez mais conectado.

1 – Mantenha o sistema operacional dos dispositivos móveis protegidos com as últimas atualizações

Esta prática oferece correções de vulnerabilidades, melhorias de segurança, compatibilidade com novos aplicativos e otimizações de desempenho, além de proteção contra malware.

2 – Faça o backup das suas informações para a segurança dos dispositivos móveis

O backup regular de informações em dispositivos móveis é crucial para garantir segurança, pois previne a perda de dados devido a danos físicos, falhas de software ou roubo.

3 – Busque fontes confiáveis para garantir dispositivos móveis protegidos

É crucial garantir que os aplicativos sejam baixados de fontes confiáveis, pois marketplaces não são infalíveis, como evidenciado pela distribuição de uma versão fake do **WhatsApp** em 2017.

4 – Utilize senha de bloqueio de tela

O bloqueio de tela com senha serve como uma barreira inicial contra acessos não autorizados em dispositivos móveis.

5 – Tenha cuidado com a exposição da sua tela

Adote o uso de uma película de privacidade e precaução em relação ao uso de mensagens de áudio em modo viva-voz, que podem expor informações confidenciais de forma inadvertida.

6 – Mantenha o antivírus atualizado para a segurança em dispositivos móveis

As atualizações frequentes adicionam definições de novos malwares à base de dados, melhorando os algoritmos de detecção e garantindo a proteção contra ameaças mais recentes.

7 – Tenha atenção ao utilizar Wi-Fi públicos para garantir seus dispositivos móveis protegidos

Redes Wi-Fi públicas são convenientes, porém, frequentemente inseguras, expondo usuários a riscos como acesso não autorizado a dados pessoais e bancários.

8 – Configure adequadamente as notificações com tela bloqueada

Notificações na tela bloqueada de dispositivos móveis podem revelar informações pessoais e sensíveis, expondo usuários a riscos de privacidade e ataques de engenharia social.

9 – Esteja consciente sobre as informações armazenadas nos dispositivos móveis

É crucial estar ciente das informações pessoais e profissionais armazenadas em dispositivos móveis para evitar consequências devastadoras em caso de perda ou roubo.

10 – Habilite o recurso de bloqueio e limpeza remoto

O recurso de bloqueio e limpeza remoto é essencial para a segurança de dispositivos móveis, garantindo a proteção de informações sensíveis.

Ferramentas de proteção cibernética

São diversas as ferramentas de proteção cibernética, incluindo firewall, softwares de monitoramento, sistemas de controle de acesso, protocolos de segurança e criptografia, além de backup inteligente.

Ferramenta	Explicação
Firewall	Uma barreira de segurança que monitora e controla o tráfego de rede, bloqueando acessos não autorizados
Softwares de monitoramento	Programas que monitoram atividades em computadores e redes, identificando padrões incomuns ou ameaças
Sistemas de controle de acesso	Ferramentas que regulam quem tem permissão para acessar determinados recursos ou áreas dentro de uma rede
Protocolos de segurança	Conjuntos de regras e procedimentos que garantem a integridade e a confidencialidade dos dados transmitidos
Criptografia	Processo de codificação de informações de forma a torná-las ilegíveis para usuários não autorizados, garantindo a segurança das comunicações
Backup inteligente	Estratégia de cópia de segurança que identifica e armazena os dados mais críticos e importantes automaticamente, impedindo perdas de dados

Essas ferramentas ajudam a identificar atividades suspeitas, bloquear malwares, restringir acesso não autorizado, criptografar dados sensíveis e realizar backups para garantir a segurança das informações da empresa.

Enquanto essas ferramentas oferecem uma camada essencial de proteção cibernética, sua eficácia pode variar dependendo da configuração e da capacidade de adaptação a novas ameaças. Além disso, a acessibilidade dessas soluções pode representar um desafio para algumas empresas, especialmente para as de pequeno porte, que podem ter recursos limitados para investir em tecnologia de segurança robusta. Portanto, é importante considerar cuidadosamente as necessidades e os recursos disponíveis ao selecionar e implementar ferramentas de proteção cibernética.

Seguros

Seguros desempenham um papel essencial na mitigação dos riscos financeiros associados a eventos imprevisíveis, fornecendo uma rede de segurança financeira em caso de perda ou dano. Especificamente em relação à segurança cibernética, os seguros podem cobrir uma variedade de situações, como violações de dados, ataques de *ransomware*, custos legais e de investigação e até mesmo perda de receita devido a interrupções no negócio. Ter um seguro adequado pode oferecer tranquilidade a empresas e indivíduos, ajudando-os a lidar com as consequências financeiras adversas de incidentes de segurança cibernética.

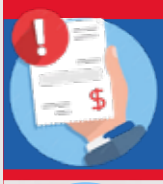
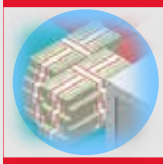
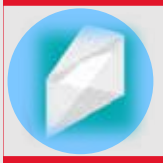
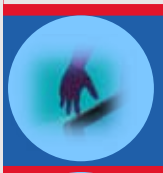
Combater e prevenir fraudes

Tipos Comuns de Fraudes Financeiras / Conscientização sobre Golpes e Esquemas Fraudulentos

De acordo com o artigo "**11 tipos de fraudes financeiras para ficar ligado!"**, do site https://www.bv.com.br/bv-inspira/golpes/tipos-de-fraudes-financeiras , podemos citar alguns dos tipos de fraudes financeiras mais aplicáveis. Veja um resumo deles a seguir.

Proteja-se contra fraudes financeiras

Não caia em golpes financeiros! Saiba como se proteger contra fraudes comuns que podem ameaçar suas finanças e dados pessoais.

	Como acontece	Como se prevenir
 **Boleto falso**	Fraudadores enviam boletos falsificados por e-mail ou mensagens, alegando dívidas inexistentes.	Desconfie de boletos fora do prazo, instale antivírus, prefira emitir boletos em sites confiáveis e verifique os dados antes do pagamento.
 **Depósito antecipado**	Para liberação de empréstimos e financiamentos, empresas fraudulentas solicitam pagamentos adiantados para aprovar créditos fictícios.	Recuse ofertas por telefone, verifique certificados de segurança, consulte a regularidade da empresa, pesquise opiniões de clientes.
 **Cartão de crédito**	Criminosos solicitam dados bancários, duplicam compras ou criam sites falsos para roubar informações	Use senhas complexas, verifique a fatura diariamente, não forneça o cartão a terceiros, ative confirmação de compras, não salve dados em sites desconhecidos, opte por seguro de cartão e bloqueie-o em caso de perda.
 **Phishing**	Golpistas enviam mensagens ou e-mails enganosos para obter informações pessoais.	Desconfie de mensagens alarmantes, bloqueie e denuncie spam, evite clicar em links suspeitos e verifique canais oficiais.
 **Investimento falso**	Também chamada de pirâmide financeira, onde ofertas de lucro rápido em investimentos inexistentes, que dependem da entrada de novos investidores.	Pesquise a idoneidade do negócio, consulte clientes e escolha empresas conceituadas.
 **Golpes no WhatsApp**	Criminosos clonam números e solicitam dinheiro a contatos próximos ou enganam usuários para obter códigos de acesso.	Ative a verificação em duas etapas, desconfie de pedidos de dinheiro, não clique em links suspeitos e não compartilhe senhas.
 **Transações com criptomoedas**	Ofertas de novas criptomoedas inexistentes ou corretoras falsas.	Conheça o mercado, desconfie de promessas exageradas, proteja seus dados e invista em criptomoedas reconhecidas.
 **Golpe do brinde**	Golpistas se passam por entregadores de brindes para obter dados pessoais.	Desconfie de contatos fora dos canais oficiais e evite fornecer dados pessoais.
 **Golpe da mão fantasma**	Golpistas enviam links para instalar malware nos dispositivos	Cautela ao abrir links e manter sistemas atualizados
 **Golpe do anúncio falso**	Anúncios falsos em redes sociais ou sites para obter informações sensíveis.	Evite clicar em links suspeitos, verifique a autenticidade dos anúncios e não compartilhe informações sensíveis.
 **Golpe do amor**	Criminosos criam perfis falsos em sites de relacionamento para solicitar dinheiro.	Mantenha ceticismo em interações on-line, desconfie de pedidos de dinheiro e evite compartilhar informações financeiras

Permaneça vigilante! Ao conhecer os principais tipos de fraudes e adotar medidas preventivas, você pode proteger suas finanças e dados pessoais contra ameaças.

Prática de prevenção de fraudes

Como pode-se ver nesta cartilha, as práticas de prevenção de fraudes abrangem medidas como proteger informações pessoais, monitorar contas bancárias e adotar medidas de segurança on-line. Isso inclui utilizar senhas fortes e únicas, habilitar a autenticação de dois fatores e monitorar, regularmente, atividades financeiras em busca de transações suspeitas. Também é crucial ter cautela ao lidar com sites e mensagens suspeitas, evitando clicar em links desconhecidos e compartilhar informações em redes Wi-Fi públicas. Essas práticas proativas ajudam a reduzir o risco de se tornar vítima de fraudes financeiras.

Uso seguro de cartões de crédito, débito e PIX

Uma experiência financeira segura e livre de fraudes com o uso de cartões de débito, crédito e PIX envolve uma combinação de práticas preventivas, conscientização e uso responsável desses métodos de pagamento eletrônico.

Cartão de débito:

Segurança: o cartão de débito oferece segurança adicional, pois o dinheiro está na conta corrente e não na carteira. Em caso de roubo ou perda, é possível bloquear o cartão imediatamente para evitar transações não autorizadas.

Monitoramento de gastos: utilize os aplicativos dos bancos para acompanhar os gastos feitos com o cartão de débito, mantendo um controle rigoroso das transações e identificando qualquer atividade suspeita.

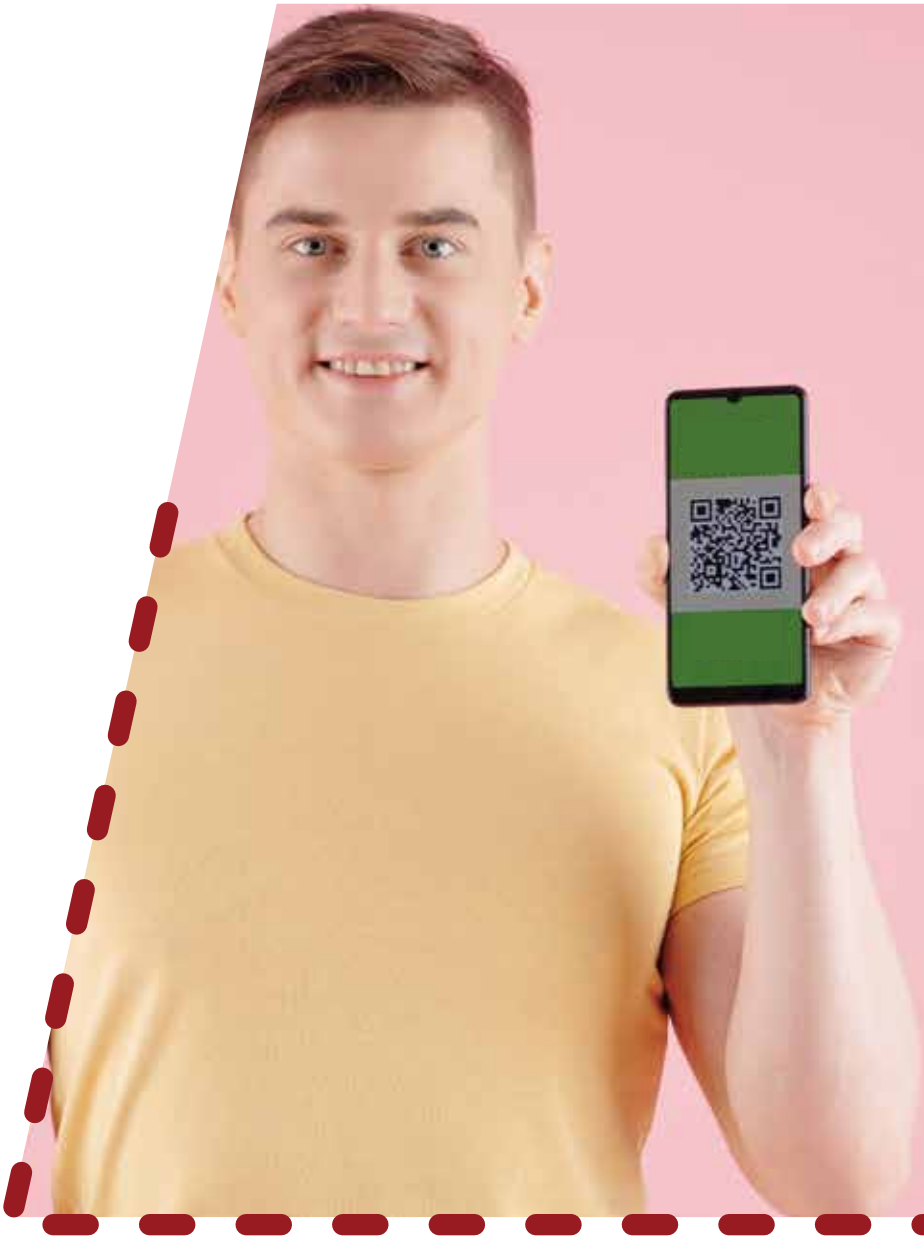
Limite de gastos: como as transações são vinculadas diretamente à conta corrente, o uso do cartão de débito pode ajudar a manter um controle mais rigoroso dos gastos, evitando o acúmulo de dívidas.

Cartão de crédito:

Proteção contra fraudes: muitos cartões de crédito oferecem proteção contra fraudes, de forma que o titular do cartão não é responsável por transações não autorizadas. É importante relatar imediatamente qualquer atividade suspeita ao emissor do cartão para evitar responsabilidade por eventuais fraudes.

Monitoramento da fatura: ao receber a fatura do cartão de crédito, revise todas as transações e garanta que sejam reconhecidas. Qualquer atividade suspeita deve ser relatada imediatamente ao emissor do cartão para investigação.

Uso responsável: o uso responsável do cartão de crédito envolve pagar o saldo integral da fatura dentro do prazo de vencimento para não pagar juros elevados. Evitar o uso excessivo do crédito e manter o saldo dentro do limite estabelecido são práticas importantes para uma experiência financeira segura.



PIX:

Autenticação segura: o PIX oferece um método de pagamento rápido e conveniente, mas é essencial garantir a autenticação segura das transações. Utilizar senhas seguras e autenticação em duas etapas, quando disponível, pode ajudar a prevenir acessos não autorizados.

Verificação de dados: ao realizar uma transferência PIX, é importante verificar, cuidadosamente, os dados do destinatário para garantir que a transação seja enviada para a pessoa ou empresa correta. Erros de digitação podem resultar em transferências acidentais para terceiros.

Evitar links suspeitos: evite clicar nesses links ao receber solicitações de pagamento via PIX. Verifique a autenticidade da fonte antes de fornecer informações pessoais ou financeiras, pois golpistas podem se passar por instituições legítimas para obter dados confidenciais.

Educação sobre engenharia social

O artigo "**Fraudes financeiras: maioria é por meio de engenharia social**" (https://www.folhavitoria.com.br/geral/noticia/11/2023/fraudes-financeiras-maioria-e-por-meio-de-engenharia-social), do site Folha Vitória, destaca que a maioria das fraudes e dos golpes financeiros é resultado da engenharia social. Essa tática visa manipular pessoas para obter informações confidenciais ou ganhos financeiros. Enquanto sistemas de segurança robustos protegem contra invasões, a engenharia social explora a confiança ou o medo das pessoas para alcançar objetivos maliciosos.

Fernando Bryan Frizzarin, especialista em cibersegurança da BluePex® Cybersecurity, cita que é necessário estar ciente dessas ameaças e técnicas para adotar posturas e práticas de segurança, como a verificação cuidadosa de toda comunicação, que envolve e-mail, telefonemas e mensagens. As empresas também devem estar atentas, pois o elo mais fraco de toda segurança digital são as pessoas.

O especialista explicou os tipos de informações mais visadas pelos fraudadores, destacando que eles têm como alvo principal dados como login e senha, informações financeiras – números de cartão de crédito, dados bancários e códigos de verificação –, documentos pessoais, endereços, dados profissionais e empresariais, informações de saúde, além de segredos comerciais e propriedade intelectual. Esses criminosos também podem selecionar suas vítimas com base em dados vazados de empresas, utilizando informações sensíveis como endereços físicos e de e-mail, dados documentais e até mesmo detalhes sobre saúde e finanças, que não deveriam estar publicamente disponíveis.

Os diferentes métodos cibercriminosos

Phishing	E-mails ou mensagens falsas que solicitam informações.
Pretexting	Criação de histórias, informações ou notícias falsas para obter dados pessoais.
Engenharia reversa	Análises de dados abertos em redes sociais para, por exemplo, criação de perfis falsos.
Manipulação psicológica e engenharia social off-line	Quando há acesso a instalações físicas, ou seja, o invasor atua pessoalmente no alvo.

IA Imitadora: Os Riscos de Solicitações Financeiras Falsas por Voz e Imagem

Uma nova abordagem de fraude digital, com sérias ramificações para a segurança financeira, é a utilização de Inteligência Artificial para imitar pessoas, tanto em voz quanto em imagem, a fim de solicitar transferências, pagamentos e outras transações fraudulentas.

A prática de usar inteligência artificial (IA) para imitar uma pessoa em imagem e voz envolve o uso de técnicas avançadas de aprendizado de máquina e processamento de linguagem natural. Para criar uma imitação convincente, os desenvolvedores alimentam algoritmos de IA com grandes conjuntos de dados contendo gravações de voz e imagens da pessoa que desejam imitar. Esses conjuntos de dados são usados para treinar modelos de IA que podem gerar novas gravações de voz e imagens que se assemelham à pessoa original. Com o avanço da tecnologia, os resultados podem ser surpreendentemente realistas, dificultando a distinção entre a imitação e a voz ou imagem reais. Uma vez criadas as imitações, os criminosos podem usá-las para enganar as vítimas, solicitando transferências de dinheiro, pagamentos ou fornecendo informações confidenciais, aproveitando-se da confiança que as pessoas têm na autenticidade das comunicações por voz ou vídeo. Essa prática ressalta a importância de fortalecer as medidas de segurança cibernética e de conscientizar o público sobre os perigos associados ao compartilhamento de informações pessoais em ambientes digitais.

Como se proteger?

Para empresas:

- Conscientização e treinamento dos funcionários;
- Implementação de políticas de segurança;
- Estabelecimento de procedimentos para verificação de identidade;
- Aprimoramento da segurança de e-mails, como inserção de filtros de spam e bloqueio de mensagens suspeitas;
- Adoção de controles de acessos a informações sensíveis e sistemas críticos;
- Monitoramento de redes e sistemas para detecção de atividades suspeitas;
- Atualização constante de sistemas operacionais e softwares para mitigar possíveis vulnerabilidades;
- Realização de backup regular de dados;
- Estabelecimento de política para uso seguro de mídias sociais;
- Plano para resposta rápida a incidentes e implantação de auditorias de segurança;
- Implementação de autenticação de dois fatores para adicionar uma camada extra de segurança;
- Uso de solução de segurança de *endpoint* que possua funcionalidades de antivírus para detectar e bloquear ameaças;
- Monitoramento do comportamento do usuário para identificar atividades incomuns.

Um endpoint é um dispositivo, como um computador ou smartphone, que está conectado a uma rede e é protegido por uma solução de segurança, como um antivírus, para detectar e bloquear ameaças cibernéticas.

Para pessoas físicas:

- Conscientização sobre a importância da segurança cibernética;
- Utilização de autenticação de dois fatores sempre que possível;
- Evitar clicar em links suspeitos ou de remetentes desconhecidos;
- Manter os dispositivos e softwares sempre atualizados;
- Fazer backup regular dos dados pessoais;
- Ser cauteloso ao compartilhar informações pessoais em redes sociais;
- Utilizar senhas fortes e únicas para cada conta on-line;
- Desconfiar de solicitações de informações confidenciais por e-mail ou telefone.

Recursos de apoio e suporte

Desempenham um papel crucial na luta contra a fraude financeira, oferecendo orientação e assistência para vítimas ou suspeitos.

Aqui estão algumas fontes de ajudam em casos de suspeita de fraude financeira:

- **Linhas diretas de assistência: muitas instituições financeiras oferecem linhas diretas de assistência dedicadas a lidar com questões de segurança e fraudes, com profissionais treinados disponíveis para fornecer orientação sobre como proceder nesses casos.**
- **Organizações de proteção ao consumidor: existem várias organizações sem fins lucrativos dedicadas à proteção dos consumidores contra fraudes financeiras. Essas organizações fornecem recursos educacionais, orientações práticas e até mesmo assistência jurídica. Elas também podem ajudar a encaminhar casos para as autoridades competentes, se necessário.**
- **Bancos e instituições financeiras: além das linhas diretas de assistência, bancos e instituições financeiras geralmente têm políticas e procedimentos estabelecidos para lidar com fraudes. Os clientes devem entrar em contato imediatamente ao detectar qualquer atividade suspeita em suas contas.**

É essencial que os consumidores conheçam e saibam como acessar os recursos de apoio e suporte disponíveis para lidar com fraudes. Agir prontamente ao detectá-las pode minimizar os danos e aumentar as chances de recuperar os ativos perdidos.

Promover a segurança da informação:

Conscientização sobre a importância da segurança da informação

Por que é importante para o setor financeiro?

Para os líderes financeiros, a segurança dos dados é crucial, pois lidam com informações confidenciais de clientes e transações comerciais. Proteger esses dados é vital para manter a confiança dos clientes, seguir regulamentos e preservar a reputação empresarial.

Ameaças atuais

Hoje, a segurança da informação é crucial para o mercado financeiro. Em 2023, as ameaças de violação de dados e ataques cibernéticos aumentaram muito. Isso pode causar grandes prejuízos financeiros e danos à reputação das empresas, além de expô-las a processos judiciais.

Quem precisa mais?

Clientes com muito dinheiro investido e aqueles que usam muito serviços digitais precisam muito de segurança. Isso inclui investidores institucionais, empresas e pessoas físicas ricas, **bem como aqueles que usam serviços bancários on-line com frequência**.

Práticas de segurança de dados pessoais/Gestão de senhas e credenciais de acesso

A senha pessoal é crucial para proteger dados financeiros on-line, servindo como uma barreira contra acessos não autorizados. Manter senhas fortes e únicas ajuda a mitigar o risco de exposição a ameaças cibernéticas, garantindo a segurança dos ativos financeiros e da privacidade on-line.

De acordo com o livro "**Boas práticas em segurança da informação**" (TCU, 2012), veja algumas dicas para criar e proteger sua senha pessoal.

Quais as melhores orientações em relação às senhas?

- Manter a confidencialidade;
- Não as compartilhar;
- Evitar registrá-las em papel;
- Criar senhas de boa qualidade, evitando que sejam muito curtas ou muito longas – que o obrigue a escrevê-las em um pedaço de papel para não serem esquecidas (recomenda-se tamanho entre seis e oito caracteres);
- Alterá-las sempre que existir qualquer indicação de possível comprometimento do sistema ou delas mesmas;
- Alterá-las em intervalos regulares ou com base no número de acessos (as senhas para usuários privilegiados devem ser alteradas com maior frequência que as normais);
- Evitar reutilizá-las;
- Alterar senhas temporárias no primeiro acesso ao sistema;

Que tipos de senhas devem ser evitadas?

Os usuários devem evitar senhas compostas de elementos facilmente identificáveis por possíveis invasores, como por exemplo:

- Nome do usuário;
- Identificador do usuário (ID), mesmo que os caracteres estejam embaralhados;
- Nome de membros de sua família ou de amigos íntimos;
- Nomes de pessoas ou lugares em geral;
- Nome do sistema operacional ou da máquina que está sendo utilizada;
- Nomes próprios;

- Datas;
- Números de telefone, de cartão de crédito, de carteira de identidade ou de outros documentos pessoais;
- Placas ou marcas de carro;
- Palavras que constam de dicionários em qualquer idioma;
- Letras ou números repetidos;
- Letras seguidas do teclado do computador (ASDFG, YUIOP);
- Objetos ou locais que podem ser vistos a partir da mesa do usuário (nome de um livro na estante, nome de uma loja vista pela janela);
- Qualquer senha com menos de 6 caracteres.

Como escolher uma boa senha?

Geralmente uma senha é considerada boa quando inclui, na composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando mais de seis caracteres. Porém, para ser boa mesmo, tem que ser difícil de ser adivinhada por outra pessoa, mas de fácil memorização, para que não seja necessário anotá-la em algum lugar. Também é conveniente escolher senhas que possam ser digitadas rapidamente, dificultando que outras pessoas, a certa distância ou por cima dos ombros, possam identificar a sequência de caracteres.

Um método bastante difundido hoje em dia é selecionar uma frase significativa para o usuário e utilizar os primeiros caracteres de cada palavra que a compõe, inserindo símbolos entre eles.

É também recomendável não utilizar a mesma senha para vários sistemas. Se um deles não for devidamente protegido, ela poderá ser descoberta e utilizada nos sistemas que, *a priori*, estariam seguros.

Se você realmente não conseguir memorizá-la e tiver que escrevê-la em algum pedaço de papel, tenha o cuidado de não identificá-la como sendo uma senha. Não pregue esse pedaço de papel no próprio computador, não a guarde junto com a sua identificação de usuário e nunca a envie por e-mail ou armazene em arquivos do computador.

Segurança de redes Wi-Fi e conexões on-line

Ao usar redes Wi-Fi públicas, é essencial proteger os dados pessoais contra ameaças potenciais. Evite acessar informações sensíveis – como dados bancários – em tais redes, pois são alvos fáceis para hackers. Ao conectar-se a uma rede em área externa, escolha a opção de conexão segura em rede pública em seus dispositivos para garantir medidas de segurança mais rigorosas. Certifique-se de que os sites que visita estão utilizando conexões seguras (https) e evite transações financeiras, optando por redes seguras e confiáveis. Evite acessar sites que exijam

senhas – como redes sociais ou bancos –para reduzir os riscos de exposição de informações pessoais.

Proteção contra roubos de identidade

O que é roubo de identidade?

O roubo de identidade é um crime em que um indivíduo utiliza informações pessoais de outra pessoa sem autorização para cometer fraudes ou outros crimes. Isso inclui o uso indevido de dados como nome, data de nascimento, número de Seguro Social ou cartões de crédito para abrir contas bancárias, fazer compras ou solicitar empréstimos em nome da vítima, podendo causar sérios danos financeiros e emocionais, além de afetar a reputação da vítima.

Formas de roubo de identidade na internet

Existem várias maneiras pelas quais os criminosos podem roubar sua identidade on-line, colocando em risco sua segurança financeira e pessoal. Uma das técnicas mais comuns é o *phishing*, que já vimos aqui no começo da cartilha.

Também, ao abrir anexos de e-mail, você está sujeito a baixar e instalar softwares maliciosos em seu dispositivo, os conhecidos malwares. Esses programas podem causar danos significativos, como roubo de informações pessoais ou corrupção de arquivos. **É essencial ter cautela** ao abrir anexos de e-mail, especialmente de remetentes desconhecidos, e **garantir que seu software antivírus esteja atualizado** para proteger seu dispositivo contra essas ameaças.

Além disso, o compartilhamento excessivo nas redes sociais facilita o roubo de identidade ao expor dados pessoais. Informações como nome, data de nascimento e localização podem ser usadas por criminosos para lançar ataques de engenharia social. Além disso, fotos e atualizações frequentes podem revelar pistas sobre nossa localização e hábitos, aumentando o risco de ataques direcionados. **Portanto, é essencial limitar as informações pessoais compartilhadas** e compreender as consequências do compartilhamento excessivo nas redes sociais.

Leitura crítica

É importante praticar a leitura crítica ao verificar a fonte e a veracidade das informações antes de compartilhá-las, especialmente quando se trata de proteção financeira. Muitas vezes, informações falsas ou enganosas circulam nas redes sociais e em outros meios, podendo levar a decisões financeiras prejudiciais. Portanto, ao receber notícias sobre investimentos ou dicas financeiras, é importante verificar sua confiabilidade e precisão. Ao compartilhar informações é fundamental garantir que você esteja divulgando **conteúdo confiável** e verificado, contribuindo para educar e proteger sua rede de contatos contra armadilhas financeiras.

Conteúdo confiável: o que é preciso para identificar um?

Determinar a confiabilidade de conteúdos on-line é essencial para acessar informações valiosas e precisas. Conteúdos confiáveis oferecem dados relevantes, explicações sólidas e análises que aprofundam a compreensão de um assunto. No entanto, encontrar essas fontes é desafiador na era das fake news, na qual verificar a veracidade das informações é difícil e a imparcialidade pode ser questionada.

Segundo o site Rock Content (2018), podemos citar virtudes de um conteúdo confiável. Veja algumas a seguir:

Conteúdo confiável cita suas fontes	Uma premissa chave do conteúdo confiável é citar fontes e referências externas, garantindo credibilidade e transparência. Isso ajuda a distinguir informações autênticas de possíveis plágios ou desinformação, sendo crucial na era das fake news
Há conteúdo similar por aí	Ao analisar a autenticidade de um conteúdo, buscar referências em outras fontes é essencial para confirmar sua veracidade, pois informações verdadeiras tendem a ser corroboradas por diversas fontes

A origem do conteúdo é confiável	A origem de um conteúdo, especialmente em um site confiável, contribui significativamente para sua credibilidade, pois a autoridade do veículo de mídia reflete na confiabilidade da informação
Ele é bem escrito	Conteúdos falsos frequentemente apresentam falhas lógicas e linguagem inadequada, indicando sua falta de confiabilidade
Conteúdo confiável não é exagerado	O uso constante de apelos como "acredite em mim" sugere falta de confiabilidade, já que conteúdos confiáveis geralmente citam fontes e argumentos sólidos, enquanto sites com **manchetes exageradas** tendem a carecer de compromisso com a verdade
Conteúdo confiável promete e cumpre	A coesão entre o título e o conteúdo do texto é crucial para avaliar sua confiabilidade; se não corresponde ao que promete na introdução, é uma indicação de falta de confiabilidade

É fundamental garantir a confiabilidade do conteúdo on-line, pois isso embasa nossas decisões e contribui para um ambiente de informação seguro. Devemos evitar compartilhar conteúdo duvidoso e sempre verificar a veracidade das informações. Ao sermos responsáveis na disseminação de conteúdo, promovemos um ambiente on-line mais confiável para todos.

Encerramento

Após abordar a importância de mitigar riscos financeiros cibernéticos, combater e prevenir fraudes financeiras e promover a segurança da informação, é fundamental agir proativamente para proteger dados e recursos financeiros para o bom andamento do seu negócio. Adotar medidas de segurança cibernética, como conscientização sobre práticas seguras, uso de ferramentas de proteção e investimento em seguros, pode ajudar a mitigar danos decorrentes de eventos adversos. Além disso, é crucial manter a vigilância contra fraudes, estar ciente dos tipos comuns de golpes e esquemas fraudulentos e agir rapidamente ao detectar atividades suspeitas. Ao agir dessa forma, você contribui para um ambiente digital mais seguro e protegido.

E lembre-se: Mantenha-se informado sobre golpes atuais! Este tema é atemporal.

Referências:

B10SEC. Importância da conscientização do usuário em segurança cibernética. Disponível em: https://pt.linkedin.com/pulse/import%C3%A2ncia-da-conscientiza%C3%A7%C3%A3o-do-usu%C3%A1rio-em-seguran%C3%A7a-cibern%C3%A9tica-kyiqf#:~:text=A%20conscientiza%C3%A7%C3%A3o%20do%20usu%C3%A1rio%20n%C3%A3o,pedra%20angular%20da%20seguran%C3%A7a%20cibern%C3%A9tica.

BESAFE BRASIL. 6 ferramentas de segurança da informação que sua empresa precisa ter! Disponível em: https://www.besafebrasil.com.br/6-ferramentas-de-seguranca-da-informacao-que-sua-empresa-precisa-ter/

BRASIL. Cartilha Boas práticas em segurança da Informação. Disponível em: https://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf/@@download/file/2511466.PDF

BV. 11 tipos de fraudes financeiras para ficar ligado! Disponível em: https://www.bv.com.br/bv-inspira/golpes/tipos-de-fraudes-financeiras

CONTACTA. Ameaças cibernéticas: principais tipos e como se prevenir. Disponível em: https://www.contacta.com.br/ameacas-ciberneticas-principais-tipos-e-como-se-prevenir/

EVAL DIGITAL. Segurança em dispositivos móveis – 10 passos para se proteger. Disponível em: https://eval.digital/seguranca-em-dispositivos-moveis-10-passos-para-se-proteger/

EXAME. As 5 melhores práticas de segurança digital para proteger seus dados. Disponível em: https://exame.com/future-of-money/melhores-praticas-de-seguranca-digital-para-proteger-seus-dados/

GCF GLOBAL. Segurança nas redes Wi-Fi. Disponível em: https://edu.gcfglobal.org/pt/seguranca-na-internet/seguranca-com-aparelhos-moveis/1/

IT-EAM. Entenda: como a segurança da informação tornou-se indispensável para o mercado financeiro. Disponível em: https://it-eam.com/como-a-seguranca-da-informacao-e-indispensavel-para-o-mercado-financeiro/

MICROSOFT. Como se proteger contra roubo de identidade online. Disponível em: https://support.microsoft.com/pt-br/office/como-se-proteger-contra-roubo-de-identidade-online-6019708f-e990-4894-9ca7-fdb53ee70830

ROCK CONTENT. Conteúdo confiável: o que é preciso para identificar um? Disponível em: https://rockcontent.com/br/talent-blog/conteudo-confiavel/#:~:text=Utilizamos%20essa%20express%C3%A3o%20para%20nos,melhor%20sobre%20um%20determinado%20assunto.

TERRA. Fraudes financeiras: maioria é por meio de engenharia social. Disponível em: https://www.terra.com.br/noticias/fraudes-financeiras-maioria-e-por-meio-de-engenharia-social,fdc5832f7a61d0a09e98820a4696a6287wuepcfj.html

UGT GOIÁS. Sinais de que você está sendo espionado online e como escapar! Disponível em: https://ugtgoias.com.br/noticias/sinais-de-que-voce-esta-sendo-espionado-online-e-como-escapar/.

SEBRAE

www.sebraerj.com.br
0800 570 0800
(21) 96576-7825
/sebraerj
Escuta essa, empreendedor!
www.ouvidoria.sebrae.com.br