GTER 51 | GTS 37

DESAFIOS EM **CYBER CULTURA E CONSCIENTIZAÇÃO**

C6 BANK

Anchises Moraes
@anchisesbr
@c6bank

O FATOR HUMANO

Riscos do Fator humano

70%

das fraudes estão vinculadas à **engenharia social**

Fonte: Febraban

https://portal.febraban.org.br/noticia/3522/pt-br/

Verizon Data Breach Investigations Report 2022

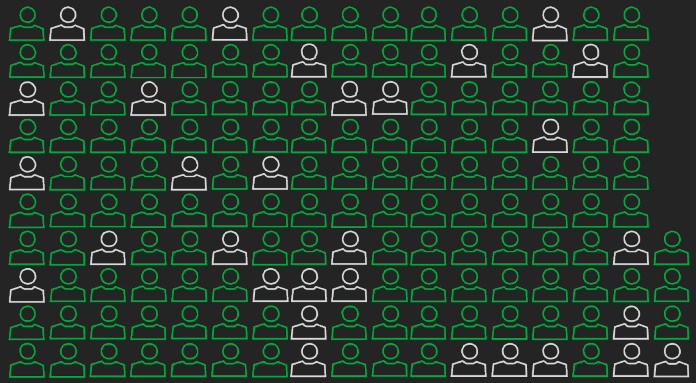


Figure 9. The human element in breaches (n=4,110)
Each glyph represents 25 breaches

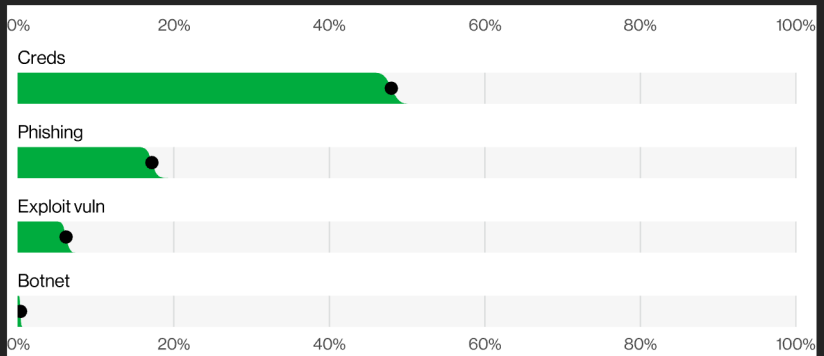


Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

https://www.verizon.com/business/resources/reports/dbir/2022/

Verizon Data Breach Investigations Report 2022

Não importa o vetor do ataque, o fator humano sempre está presente !!!

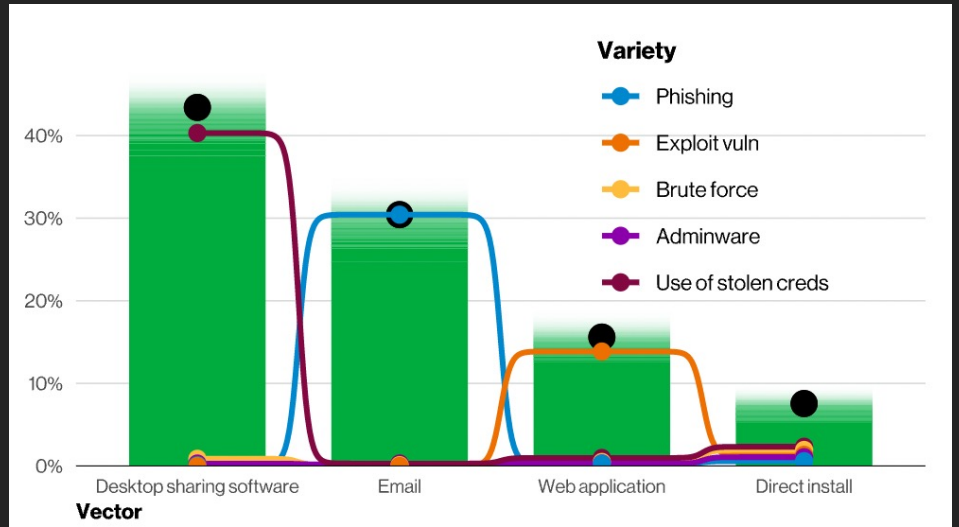


Figure 39. Select action varieties within vectors in System Intrusion Ransomware incidents (n=1,032)

https://www.verizon.com/business/resources/reports/dbir/2022/

Exemplos recentes

Hackers Breached Colonial Pipeline Using Compromised VPN Password

June 07, 2021 Ravie Lakshmanan

https://thehackernews.com/2021/06/hackers-breached-colonial-pipeline.html

Senha para VPN da Colonial Pipeline estava na dark web

Descoberta foi feita pelos peritos da Mandiant, empresa especializada em forensics, contratada pela Colonial para investigar o incidente

Da Redação
06/06/2021

https://www.cisoadvisor.com.br/senha-para-vpn-da-colonial-pipeline-estava-na-dark-web/

Exemplos recentes

Uber Comms
@Uber_Comms

We are currently responding to a cybersecurity incident. We are in touch with law enforcement and will post additional updates here as they become available.

10:25 PM · Sep 15, 2022 · Twitter Web App

REUTERS®

World Business Legal Markets More

Autos & Transportation

3 minute read · September 16, 2022 5:52 PM GMT-3 · Last Updated a month ago

Uber investigating 'cybersecurity incident' after report of breach

Reuters

(I was spamming employee with push auth for over a hour) i then contacted him on WhatsApp and claimed to be from Uber IT, told him if he wants it to stop he must accept it 6:47 PM

And well, he accepted and I added my device 6:47 PM

[redacted] Uber staff posted a comment. Sep 15th (5 mins ago)

UBER HAS BEEN HACKED (domain admin, aws admin, vsphere admin, gsuite SA) AND THIS HACKERONE ACCOUNT HAS BEEN ALSO

https://twitter.com/Uber_Comms/status/1570584747071639552
https://www.bleepingcomputer.com/news/security/uber-hacked-internal-systems-breached-and-vulnerability-reports-stolen/
https://www.reuters.com/business/autos-transportation/uber-investigating-computer-network-breach-nyt-2022-09-16/

Exemplos recentes

Oferta de trabalho falsa está por trás do hack de US$ 600 milhões

Segundo pesquisadores, esta foi a razão por trás do hacking ao Axie Infinity, o popular game em blockchain que paga criptomoedas aos jogadores

Da Redação
10/07/2022

Microsoft 365 Email Hack Led to American Airlines Breach

Airline Says July Phishing Incident Exposed Personal Information of 1,700 People

Cal Harrison • September 28, 2022

Insider Threat: Employees indicted for stealing $88 million of license keys

Posted: July 4, 2022 by Malwarebytes Labs

Hacker gang broke into Silicon Valley chipmaker AMD because of workers' terrible passwords

Joshua Bote, SFGATE
June 30, 2022

https://www.cisoadvisor.com.br/oferta-de-trabalho-falso-esta-por-tras-do-hack-de-us-600-mi%EF%BF%BClhoes/
https://www.databreachtoday.com/microsoft-365-email-hack-led-to-american-airlines-breach-a-20168

Moral da história

Devemos proteger os usuários **deles mesmos!**

CLASSIFICAÇÃO INTERNA

DESAFIOS

Desafios Atuais: PÓS-PANDEMIA

AUMENTO NAS FRAUDES

Phishing
Golpe do Falso Motoboy
Golpe do Delivery

80%

Aumento nas tentativas de **phishing**

https://portal.febraban.org.br/noticia/3441/pt-br/
https://portal.febraban.org.br/noticia/3522/pt-br/

Desafios Atuais: PÓS-PANDEMIA

RETOMADA ECONÔMICA

Golpe do Falso Emprego
Falsa Renegociação de dívidas
Sequestro de Instagram para falsa venda

Golpe com boleto bancário cresce 785% em 2021; saiba se proteger

Golpe de renegociação cresce no Brasil e induz vítimas a acreditarem que estão quitando dívidas com descontos

Por Marvin Costa, para o TechTudo
05/08/2021 06h00 · Atualizado há 3 meses

Fraude no home office: vagas de emprego falsas prometem renda diária

Por Altieres Rohr em Maio 19, 2022

Olá, sou gerente de contratação na [redacted] devido a vagas estaremos enviando uma candidatura de meio período para trabalhar em casa, o salário será pago no mesmo dia, 900-4000 reais por dia. Interessados em entrar em contato comigo para consulta no Whatsapp+55[redacted]

Clique no link para adicionar automaticamente:

Golpe no Instagram usa perfil de vítima para anunciar ofertas falsas a seguidores; veja como se proteger

Posts oferecendo eletrodomésticos e eletrônicos a preços baixos se tornaram frequentes, mas são iscas usadas por criminosos.

Por Alessandro Feitosa Jr, g1
02/02/2022 07h00 · Atualizado há 4 meses

https://blog.axur.com/pt/fraude-no-home-office-vagas-de-emprego-falsas-prometem-renda-diaria
https://www.techtudo.com.br/noticias/2021/08/golpe-com-boleto-bancario-cresce-785percent-em-2021-saiba-se-proteger.ghtml
https://g1.globo.com/tecnologia/noticia/2022/02/02/golpe-no-instagram-usa-perfil-de-vitima-para-anunciar-ofertas-falsas-a-seguidores-veja-como-se-proteger.ghtml

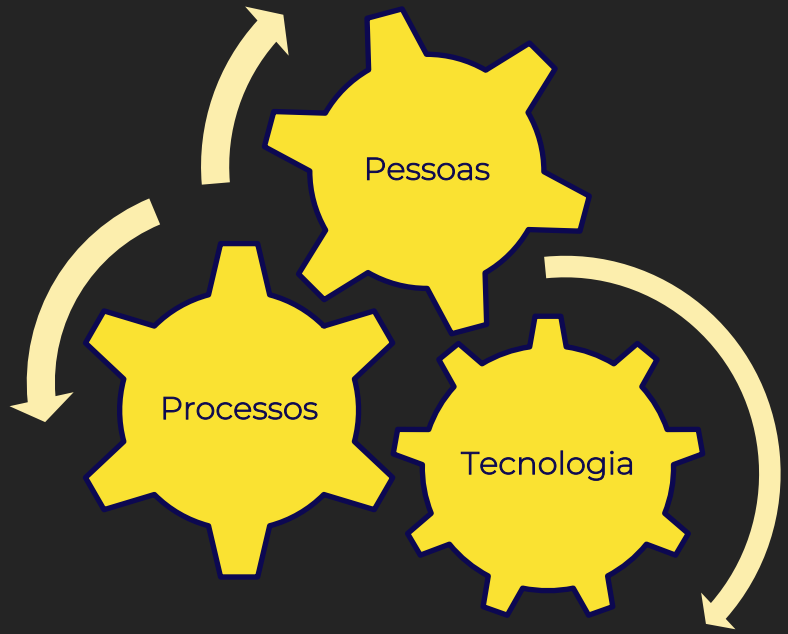
Desafios Atuais: Home Office

TRABALHO HÍBRIDO

Acesso remoto
Segurança em casa
Novas estratégias de comunicação
Novos desafios em cultura e conscientização

https://resources.digitalshadows.com/infographics/threat-model-of-a-remote-worker

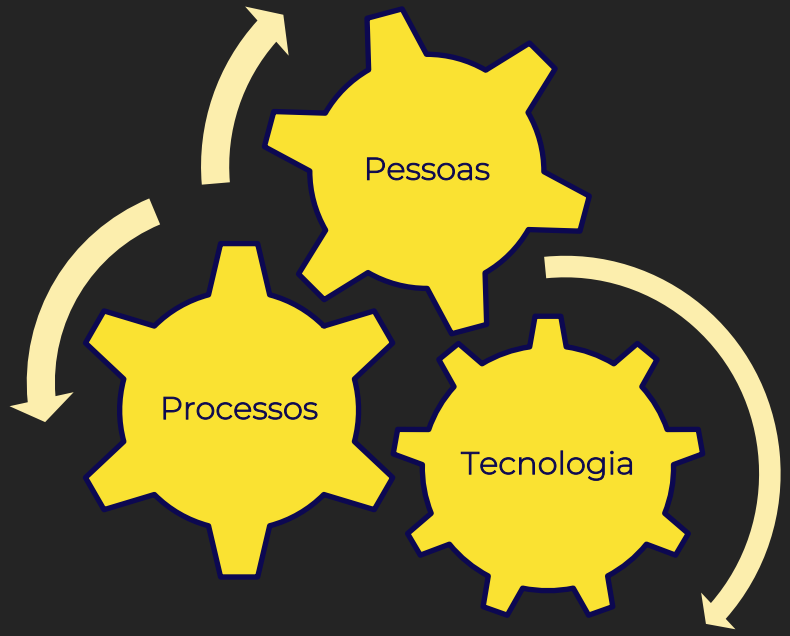
Teoria



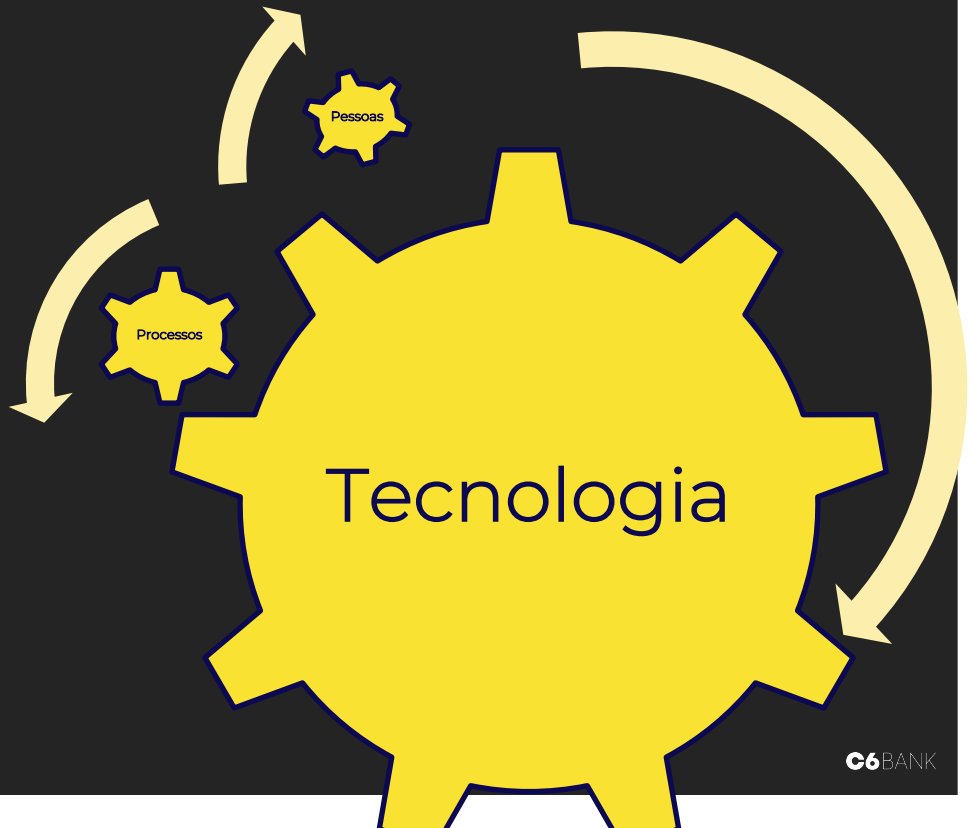
Realidade

C6BANK

Teoria



Realidade



CLASSIFICAÇÃO INTERNA

Teoria

Realidade

Bancos gastaram R$ 5,7 mi com treinamentos em cibersegurança

https://www.cisoadvisor.com.br/gastos-dos-bancos-com-treinamento-em-cibersegurança-subiu-138/

Realidade

Bancos gastaram R$ 5,7 mi com treinamentos em cibersegurança

https://www.cisoadvisor.com.br/gastos-dos-bancos-com-treinamento-em-cibersegurança-subiu-138/

O gastos totais dos bancos em tecnologia, englobando despesas e investimentos, devem atingir R$ 35,5 bilhões neste ano, o que, se confirmado, representará aumento de 18% em relação ao orçamento de 2021. É o que revela o primeiro volume da Pesquisa Febraban de Tecnologia Bancária 2022, realizada pela Deloitte, qual também indica que os investimentos em tecnologia estão direcionados ao que está no topo da agenda tecnológica das instituições financeiras: segurança cibernética, inteligência artificial, 5G, cloud e big data.

Realidade

35,5bi

Treinamentos

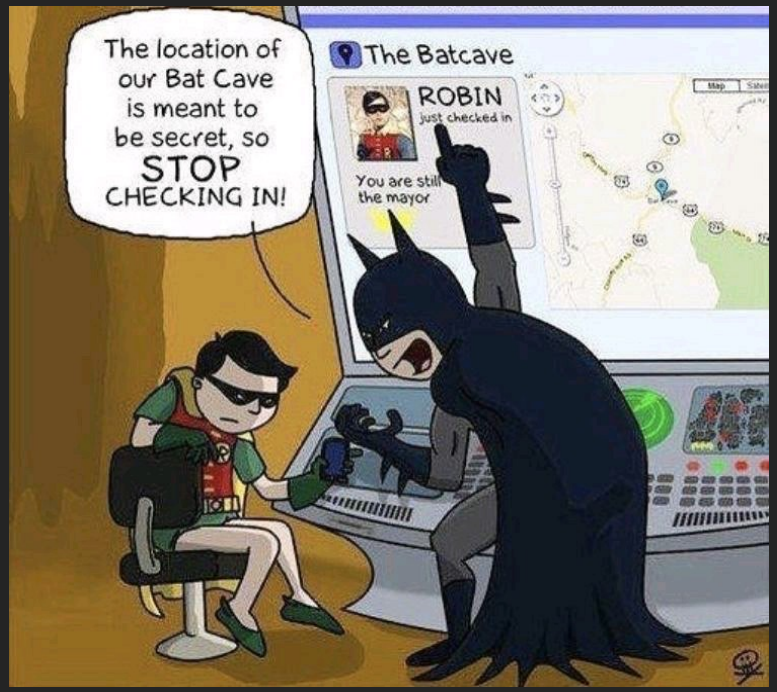
Investimento dos bancos em tecnologia em 2022 (R$)

CLASSIFICAÇÃO INTERNA

CRIANDO UMA CULTURA DE SEGURANÇA

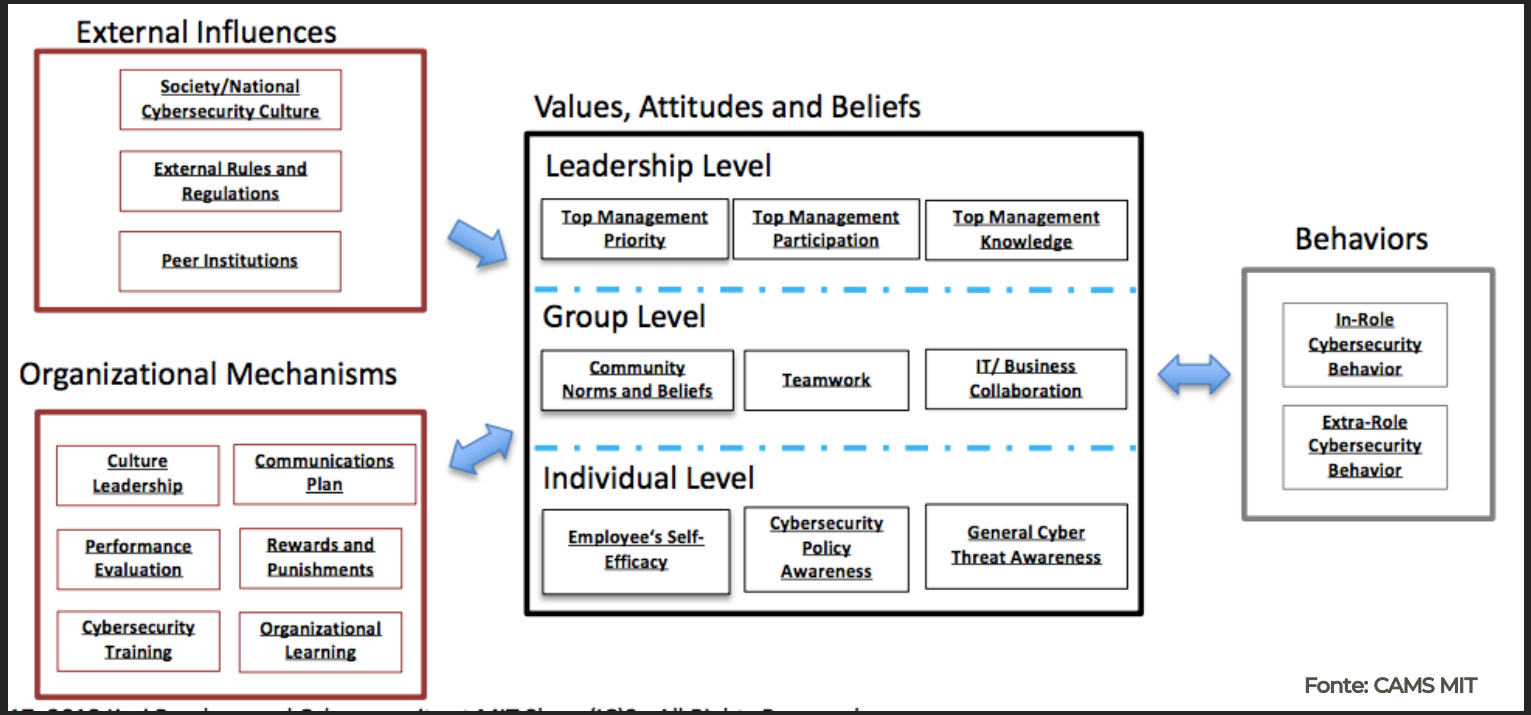
Porque?

"Tratar a ciber segurança como parte dos valores, crenças e atitudes do dia-a-dia”
(CAMS MIT)



Como?

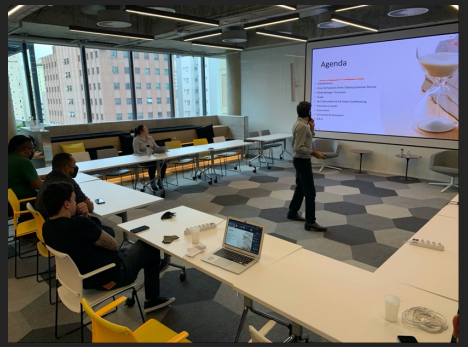
Framework for Building a Culture of Cybersecurity
https://cams.mit.edu/wp-content/uploads/Building-a-Culture-of-Cybersecurity.pdf

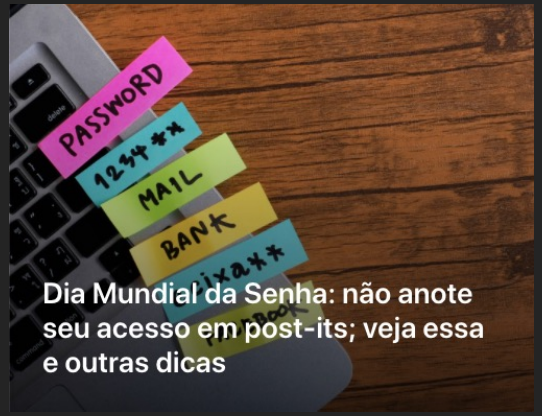


Fonte: CAMS MIT

C6BANK

Como?





Processo constante

Treinamento obrigatório anual
Ações e campanhas periódicas
Treinamentos
Testes e simulações
Gamificação
“Security Champions”

C6 BANK Intranet - C6 Bank

Início | Gente e Gestão | Transparência | Marca | Roadmap 2021 | C6 Service Desk

Seguindo

Enviar para | Leitura Avançada

LGPD Week: como a LGPD irá impactar sua vida? Faça o download da nossa cartilha

Comunicacao

Publicada em 25/08/2021

Você, certamente, já deve ter sido abordado por um atendente em uma farmácia pedindo seu CPF e informando sobre as políticas de programas para descontos em medicamentos e produtos. Ou, já recebeu mensagens com pedidos de autorização para uso de cookies em sites e aplicativos. Essas ações são consequências da LGPD (Lei Geral de Proteção de Dados Pessoais), que **cria regras para a coleta, uso, armazenamento e tratamento de dados pessoais**.

A aplicação da lei impacta em diversas relações do nosso dia a dia, como comércio e de serviços, ou seja, qualquer relação que implique o uso dessas informações. Ela determina o tratamento especial para dados como número de identidade, CPF ou e-mail, além de dados como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, religião ou partido político.

Você sabia que a LGPD tem papel muito importante no Open Banking?

Por conta da Lei Geral de Proteção de Dados Pessoais, o acesso e a portabilidade dos dados financeiros são direitos do cliente, tendo o poder de decisão sobre o compartilhamento de suas informações financeiras. Por isso, a implementação do Open Banking pelas instituições financeiras respeita diversos cuidados e usa as tecnologias existentes para garantir o consentimento e autorização no acesso às suas informações e como serão usadas.

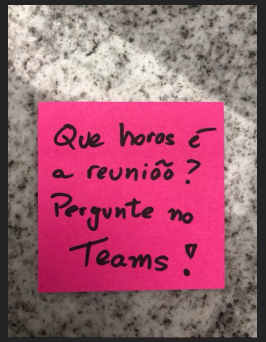
Dicas Rápidas

Apoio da Alta Gestão

Mensagem simples e objetiva

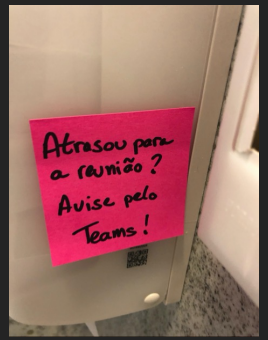
Alinhamento e apoio com demais áreas

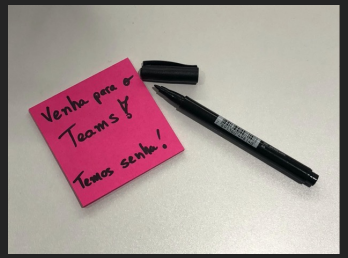
Dicas



Criatividade & bom humor

CAMPANHA “USE O TEAMS”
Post-its colados nos banheiros
do escritório

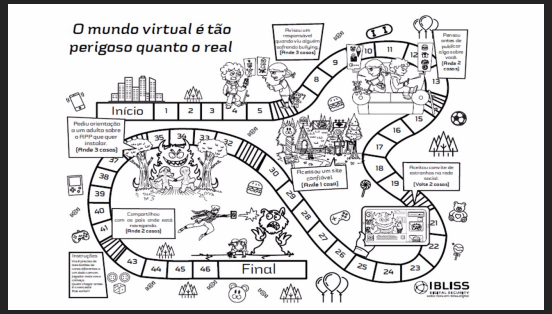




Dicas

Aproveitar datas especiais

Janeiro: Data Privacy Day
Fevereiro: Carnaval
Fev: Dia Mundial da Internet Segura (“Safer Internet Day”)
Agosto: LGPD
Out: Dia das Crianças
Out: Ada Lovelace Day
Out: Mês da Segurança
Nov: Black Friday



Mais Dicas

Foco em canais digitais

Intranet
E-mail
Vídeos
Aplicativos de comunicação
Redes sociais

C6BANK Intranet - C6 Bank

Início | Gente e Gestão | Transparência | Marca | ... | Seguindo

Enviar para

Sem dor de cabeça: confira dicas para usar o Pix com segurança

Comunicacao

Publicada em 26/04/2021

O **Pix, sistema de pagamentos instantâneos do Banco Central,** completou seis meses de operação com mais de 80 milhões de usuários cadastrados — entre pessoas físicas e jurídicas. Ele já apresenta indícios de que se tornará cada vez mais presente na vida dos brasileiros.

Por ser uma ferramenta amplamente usada pelo público para transações financeiras, o sistema chamou a atenção de criminosos e ganhou algumas modalidades de golpe. Por isso, o Banco Central do Brasil, em parceria com a Febraban e com os bancos, realiza nesta semana uma **campanha de conscientização sobre segurança do Pix**.

Intitulada de **"O Pix é novo, mas os golpes são antigos"**, a campanha tem como objetivo **alertar os cidadãos para as principais estratégias de fraudes e de engenharia social** utilizadas pelos golpistas, além de **conscientizá-los a respeito dos cuidados necessários para não serem vítimas dessas fraudes**.

Veja abaixo quais são **os quatro problemas** que acontecem com mais frequência e as **dicas para evitá-los**:

c6bank 15min

CUIDADO COM
O GOLPE DO PIX

Com a popularidade do **PIX**, criminosos têm usado esse meio de pagamento para aplicar **golpes**.

Por isso, em parceria com o **@bancocentraldobrasil** e a **@febraban_oficial** , trouxemos algumas **dicas de segurança**!

Conheça os **principais golpes**

c6bank 15min

1. SITES FALSOS
EM NOME DO PIX

Golpistas enviam por e-mail, SMS ou redes sociais, links falsos em nome do banco para a vítima realizar um cadastro ou transação do PIX a fim de roubar seus dados.

2. INVASÃO DE CONTA

Fraudador envia mensagem suspeita por SMS, WhatsApp ou por um site falso, a vítima responde e libera o acesso para sua conta bancária.

C6 Bank @C6Bank

Com a popularidade do PIX, criminosos têm usado esse meio de pagamento para aplicar golpes.

Por isso, em parceria com o @BancoCentralBR e a @FEBRABAN, trouxemos algumas dicas de segurança!

Siga a trend 👇

Translate Tweet

11:25 AM · Apr 30, 2021 · Twitter Web App

4 Retweets **40** Likes

C6 Bank @C6Bank · 1h
Replying to @C6Bank
1. SITES FALSOS EM NOME DO PIX 💻

Golpistas enviam por e-mail, SMS ou redes sociais links falsos em nome do banco para a vítima realizar um cadastro ou transação do PIX a fim de roubar seus dados.

1 · 6

C6 Bank @C6Bank · 1h
2. INVASÃO DE CONTA 📲

Fraudador envia mensagem suspeita por SMS, WhatsApp ou por um site falso, a vítima responde e libera o acesso para sua conta bancária.

1 · 6

C6 Bank @C6Bank · 1h
3. CENTRAL DE ATENDIMENTO FALSA ☎️

Golpista se passa por um atendente bancário e entra em contato para resolver assuntos de cadastro do PIX e a vítima acaba fornecendo informações de login e senha do banco.

1 · 6

C6 Bank @C6Bank · 1h
4. GOLPE DO PIX EM DOBRO 👀

Golpistas prometem devolver o valor em dobro para a sua conta se você fazer um PIX para uma "chave com problema".

1 · 6

C6 Bank @C6Bank · 1h
COMO EVITAR GOLPES

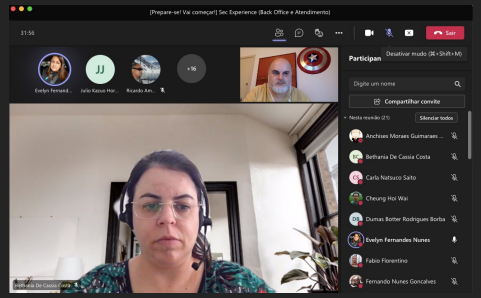
- Proteja seu acesso: crie senhas complexas e não use senhas repetidas
- Verifique a autenticidade de endereços visitados na internet
- Cadastre e faça o PIX somente pelo app do seu banco
- Não confie em promessas de dinheiro fácil

1 · 17

C6 Bank @C6Bank · 1h
Se tiver qualquer suspeita entre em contato com os canais oficiais do seu banco imediatamente.

1 · 16

Mais Dicas



Faça parte do dia-a-dia das pessoas

Ações frequentes

Coloque segurança na agenda dos times

SEC EXPERIENCE
Roadshow com diversos times para **tirar dúvidas e colher feedbacks** sobre os controles de segurança e impacto no dia-a-dia.

Mais Dicas

Métricas

Realizações e cases de sucesso

Mostrar eficiência

27
Ações realizadas

97%
Adesão aos Treinamentos Regulatórios (CSixers)

Campanha
CYBER WEEK
Febraban

12
Campanhas em redes sociais

Cartilha de Dicas de Segurança

Campanha
"João e Maria Cyber"
(Dia das Crianças)

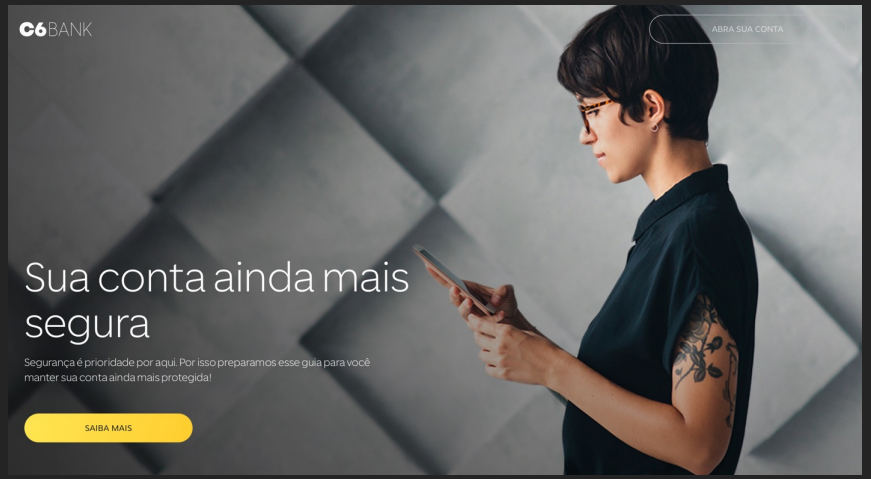
06
Meetups de Segurança

8
Turmas de Treinamentos sobre LGPD

30
Notificações e artigos na Intranet

Exemplos

https://www.c6bank.com.br/seguranca
https://www.c6bank.com.br/contasegura



Referências

Case Study “Cybersecurity Culture at C6 Bank”, MIT Sloan
https://cams.mit.edu/wp-content/uploads/Cybersecurity-Culture-at-C6-Bank-CaseStudy.pdf

Palestra “Cyber Cultura em tempos de Coronavírus” – Roadsec@Home
https://www.youtube.com/watch?v=NYOq8P6KGdY

Live "Crimes Virtuais em tempos de COVID-19" - C6 Talks
https://www.youtube.com/watch?v=R_pdQicgPSE

CLASSIFICAÇÃO INTERNA

Referências

Framework for Building a Culture of Cybersecurity, MIT Sloan
https://cams.mit.edu/wp-content/uploads/Building_Cybersecurity_Culture.pdf

Cybersecurity Culture Maturity Model
https://cams.mit.edu/wp-content/uploads/Cybersecurity_Culture_Maturity_Model.pdf

Regulamentações sobre Conscientização e Treinamento em Segurança
https://anchisesbr.blogspot.com/2020/06/seguranca-regulamentacoes-sobre.html

Datas comemorativas sobre segurança
https://anchisesbr.blogspot.com/2021/05/seguranca-datas-comemorativas-sobre.html

Dúvidas ?

OBRIGADO

Anchises Moraes
@anchisesbr
@c6bank
@bsidessp
@garoahc
@lwomcy
@csabr

C6 BANK