

CULTSEC

A NOVA ERA DA CONSCIENTIZAÇÃO

**Protegendo Sua Privacidade
Digital: Da Vida Pessoal à
Segurança Empresarial**



Dados e Informações

Como geramos dados no dia a dia



O que compartilho?

O que o Google sabe sobre mim?



Exemplos de Ataques



Como manter sua empresa segura

Bio



Leonardo La Rosa
[linkedin.com/in/leonardolarosa](https://www.linkedin.com/in/leonardolarosa)

Bio

LEONARDO LA ROSA

Mais de 25 Anos de Experiência nas áreas de TI, incluindo Infraestrutura e Cibersegurança, com atuação em diversos setores de mercado, sendo a maior parte Instituições Financeiras.

Tecnólogo em Processamento de Dados pela UNIBAN
MBA em Gestão de Tecnologia da Informação pela FIAP

• C|SCU • N|SF • C|ND • C|EH • E|CIH • C|ASE Java • C|EI • ICSI|CNSS • Lead Implementer ISO 27701 • C|CSE • C|SA • C|TIA

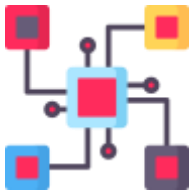
- Infrastructure e Cyber Security Director e Sócio na ACADI-TI
- DPO na ACADI-TI
- Instrutor das certificações EC-COUNCIL
- Instrutor de treinamentos próprios na ACADI-TI
- Docente do Curso de Pós Graduação em Cibersegurança Ofensiva - ACADI-TI
- Digital Influencer sobre temas relacionados a Cibersegurança
- Hardware Hacking maker (mais de 10 dispositivos criados para ataque a segurança física)
- Autor de +200 conteúdos / cursos de Cyber Security

Dados e Informações



Como conscientizar nossos times sobre segurança de dentro para fora?

Dados e Informações



Dados são um conjunto de valores ou ocorrências em um estado bruto com o qual **são** obtidas informações com o objetivo de adquirir benefícios.

Fonte: <https://pt.wikipedia.org/wiki/Dados>



Informação é a resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano, animal ou máquina) que a recebe.

Fonte: <https://pt.wikipedia.org/wiki/Informação>

Como os dados são gerados?



Um Vídeo gravado com
uma Filmadora

Um Áudio gravado no
Microfone

Uma Foto tirada no Celular

Um Download da Internet

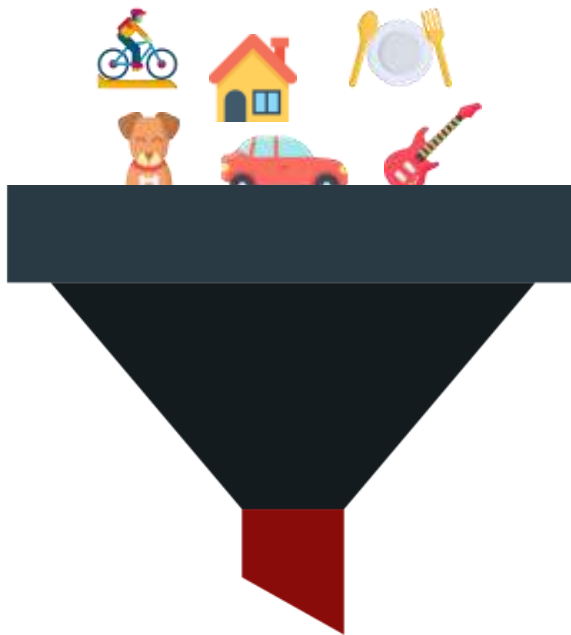
Uma Mensagem de SMS

Uma Música no Aplicativo

Um E-mail no Computador

Uma Localização no Mapa

Dados e informações



Informações facilitam as empresas a localizarem seus consumidores...



Porém, se acessados por pessoas mal intencionadas, pode resultar em ataques!



Dados e informações



O conjunto de dados pessoais, após processado, leva à informações de um determinado indivíduo.

Muitas pessoas compartilham seus dados na Internet em diversos websites, como fóruns, sites de notícias, sites de mídias sociais.

As empresas disputam sua atenção pela internet! Todos querem de alguma forma se conectar a você para vender seus serviços e produtos.

Quando uma empresa possui dados de pessoas, como perfil de consumo, interesses, sexo, idade, religião, classe financeira, etc. fica muito mais fácil direcionar as campanhas para o público desejado



Quanto valem seus dados

O valor dos dados vai muito além do financeiro!



O registro das crianças se divertindo nas férias



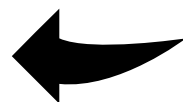
A recordação de um ente querido que partiu

Uma história “QUASE” verdadeira



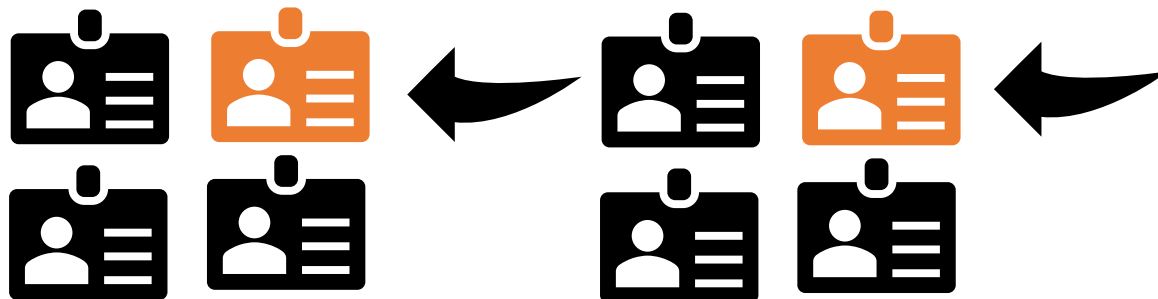
João trabalha na empresa Cyber Global Tech Brasil, uma grande empresa na área de tecnologia

Uma história “QUASE” verdadeira



O time de Recursos Humanos na Cyber Global Tech Brasil está sempre preocupado em fornecer os melhores benefícios para seus funcionários.

Uma história “QUASE” verdadeira



Recentemente, o RH foi sondado por uma academia que desejava fazer uma parceria com a empresa de João oferecendo 50% de desconto para os funcionários.

Uma história “QUASE” verdadeira



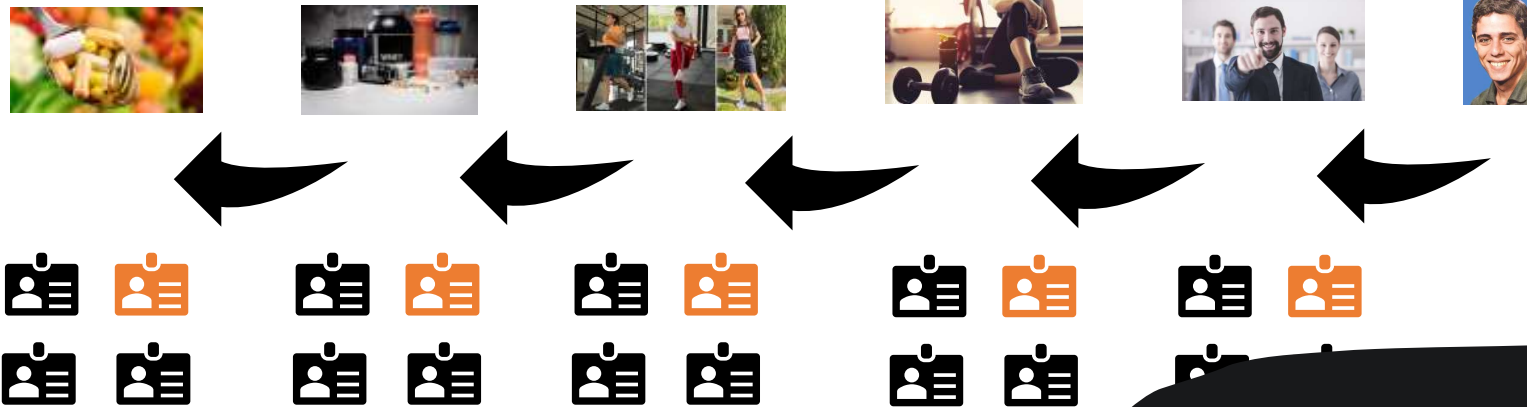
A empresa Fitness Body, que produz roupas para pessoas fitness, entrou em contato com a academia oferecendo desconto para todos os alunos.



Uma história “QUASE” verdadeira



Este ciclo continua... As empresas compartilham dados com parceiros e fornecedores e parceiros constantemente



Uma história “QUASE” verdadeira



E assim, os dados do João que deveriam ser cuidados pela empresa, passaram de empresa em empresa...

Uma história “QUASE” verdadeira



E assim, os dados do João que deveriam ser cuidados pela empresa, passaram de empresa em empresa...

Mas a culpa não é do RH



Como você se comporta em:



Nossos Dados



Minha atividade no Google.

A atividade que você guarda permite melhorar os serviços do Google, oferecendo recursos como a redescoberta do que você pesquisou, leu e assistiu.

Você pode ver e excluir sua atividade usando os controles disponíveis nesta página.

Atividade na Web e de apps	Histórico de localização	Histórico do YouTube
<input checked="" type="checkbox"/> Ativada >	<input checked="" type="checkbox"/> Ativada >	<input checked="" type="checkbox"/> Ativada >



Nossos Dados



Atividade na Web e de apps

Salva sua atividade em sites e apps do Google, incluindo informações associadas (como local), para oferecer pesquisas mais rápidas, recomendações melhores e experiências mais personalizadas no Google Maps, na Pesquisa e em outros serviços do Google. [Saiba mais](#)

☒ Ativada

[Desativar](#)

Ver e excluir atividades



Nossos Dados



Histórico de localização

Salva os locais que você visita com seus dispositivos, mesmo que não esteja usando um serviço específico do Google, para fornecer mapas personalizados, recomendações com base nos lugares visitados e muito mais. [Saiba mais](#)

☒ Ativada

Ativada desde 29 de agosto de 2023

Desativar



Nossos Dados



Histórico do YouTube

Salva os vídeos do YouTube que você assiste e as pesquisas que faz nesse serviço para oferecer recomendações melhores, lembrar onde você parou e muito mais. [Saiba mais](#)

☒ Ativada

[Desativar](#)



OSINT



OSINT (Inteligência de Fontes Abertas) é o termo usado para descrever a inteligência, no sentido de informações, como em serviço de inteligência, obtida através dados disponíveis para o público em geral, como jornais, revistas científicas e emissoras de TV.

OSINT é uma das fontes de inteligência. É conhecimento produzido através de dados e informações disponíveis e acessíveis a qualquer pessoa

OSINT



rl34075
LaRosa Leonardo

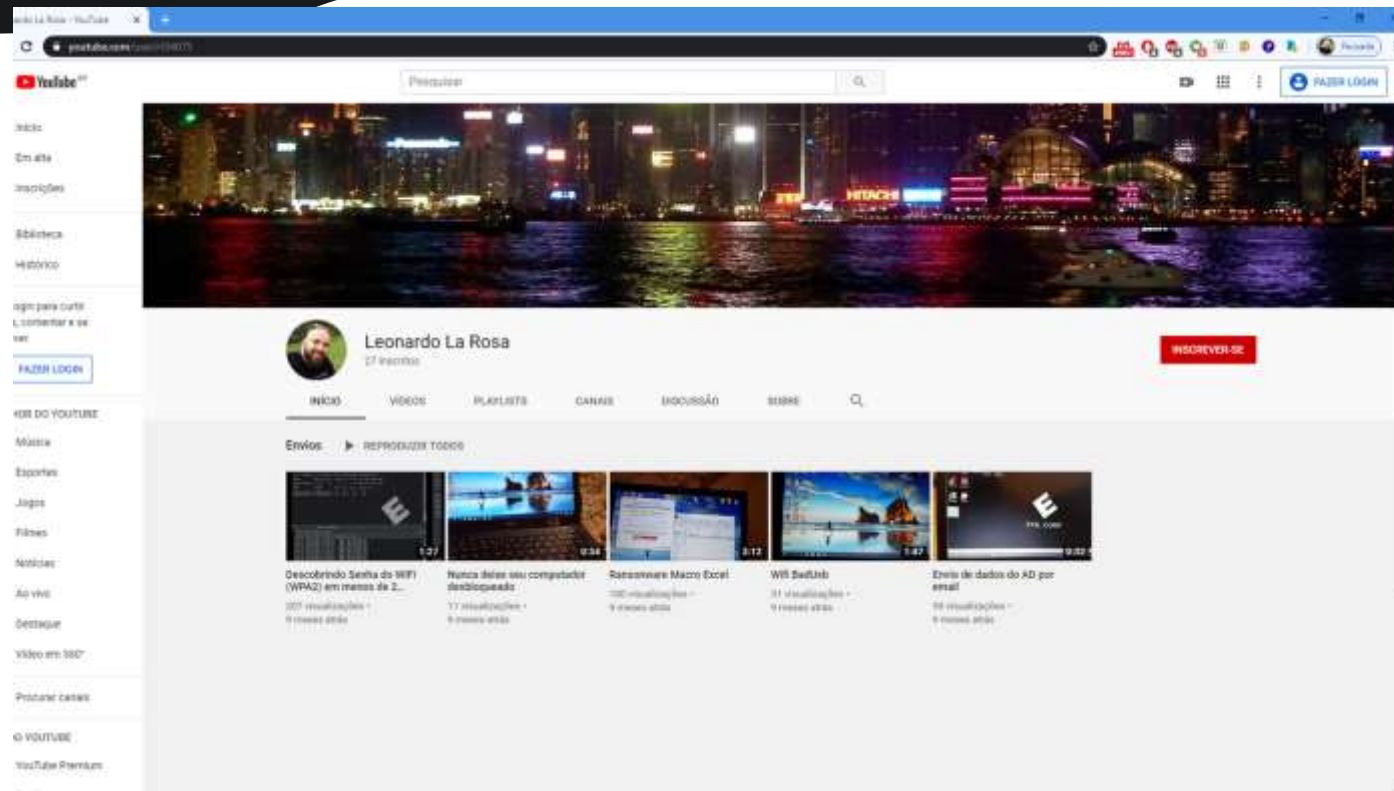
Seguindo

OSINT

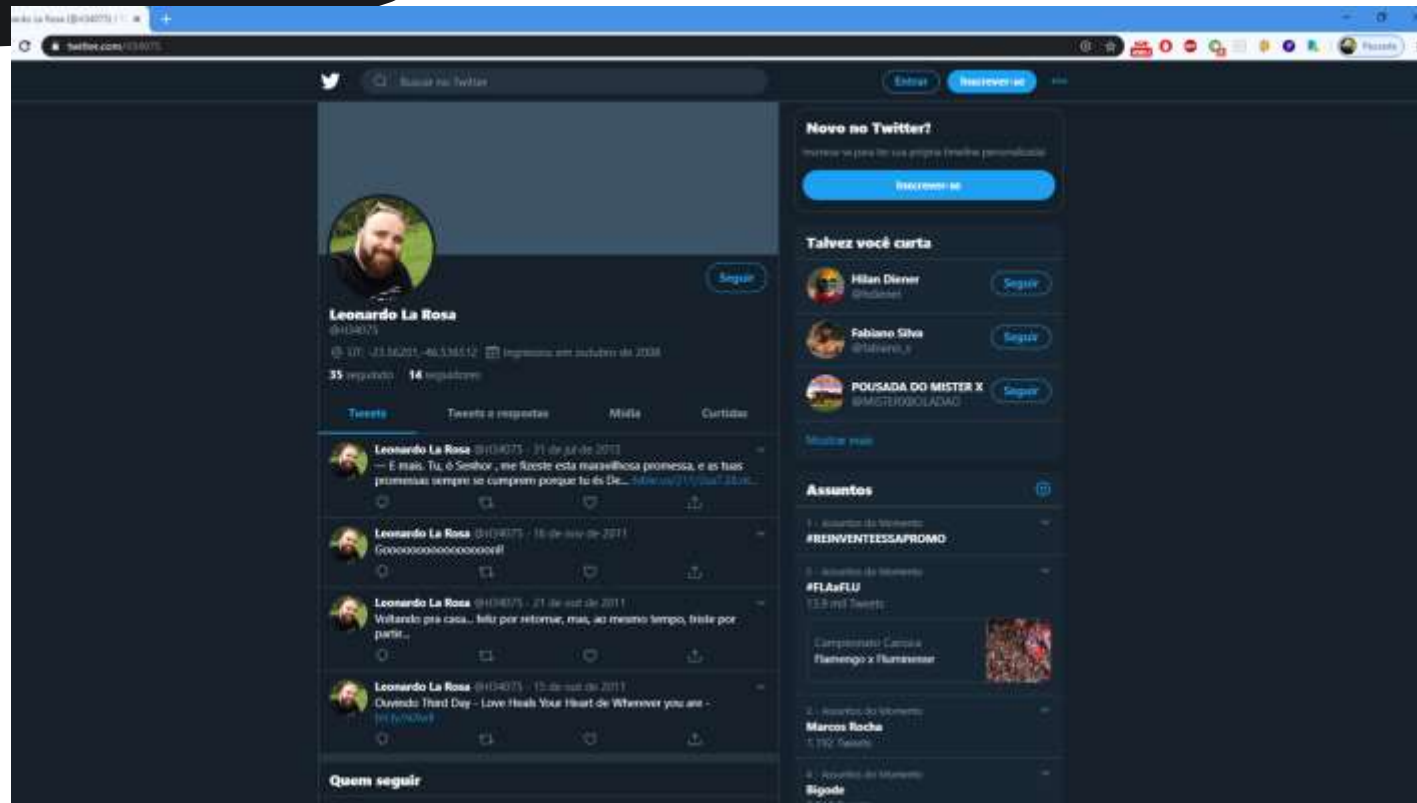


<https://checkusernames.com/>

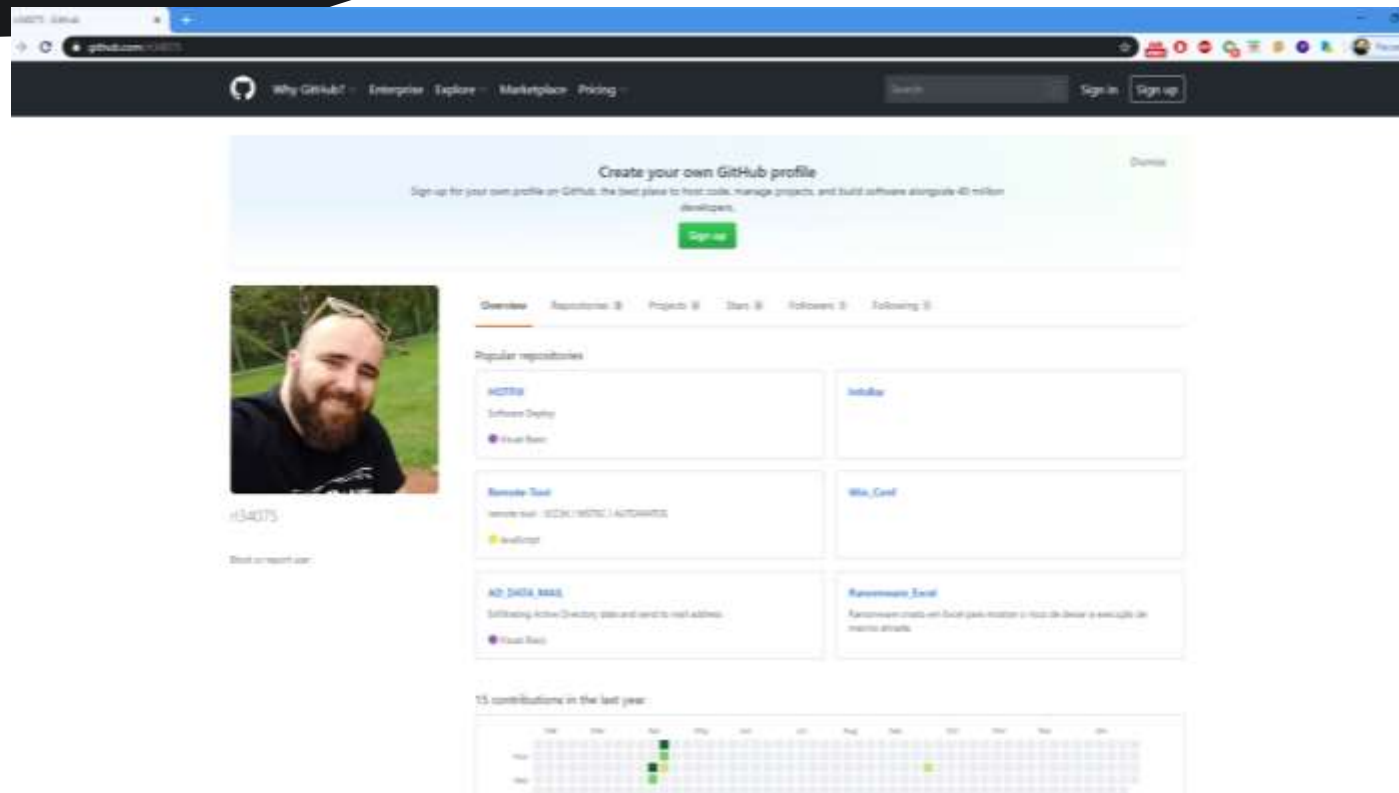
OSINT



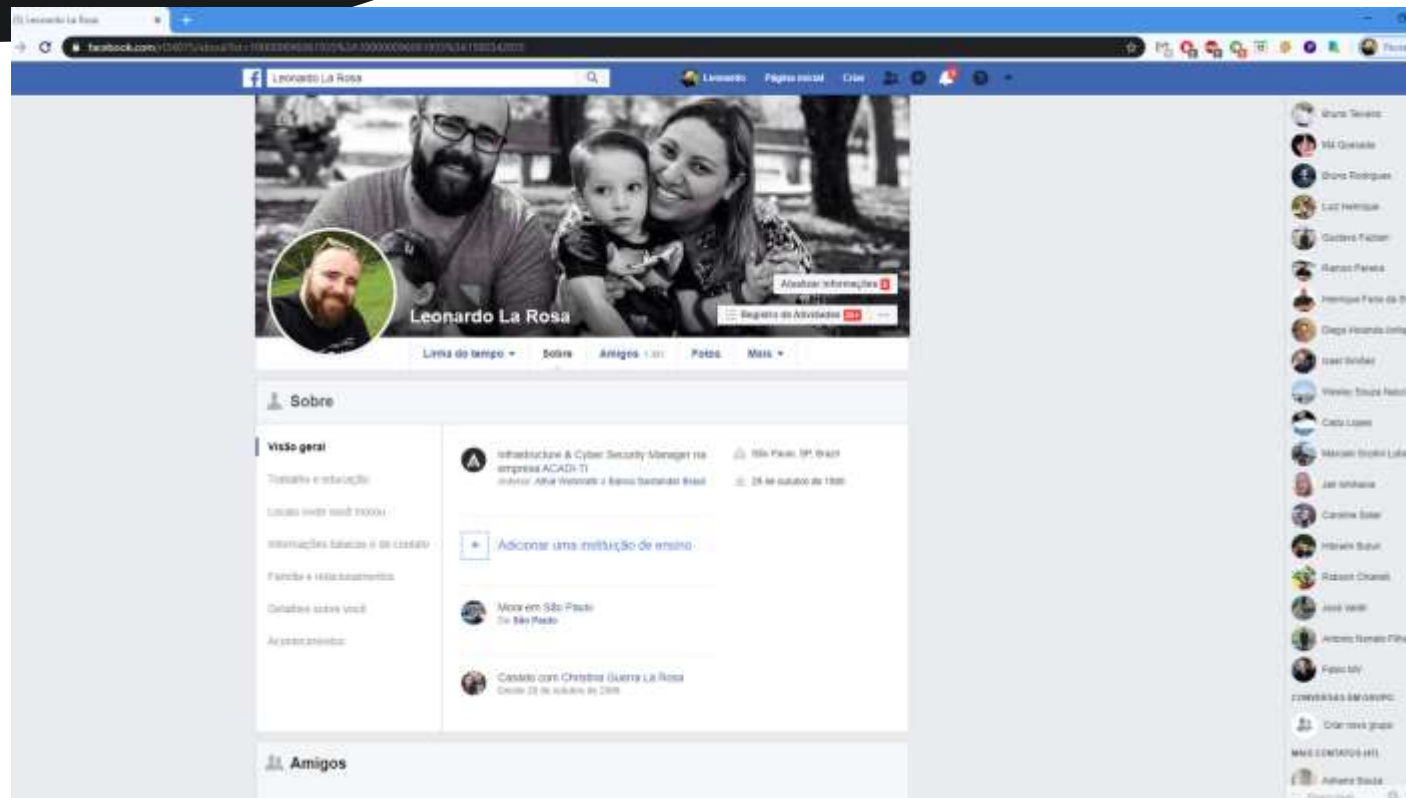
OSINT



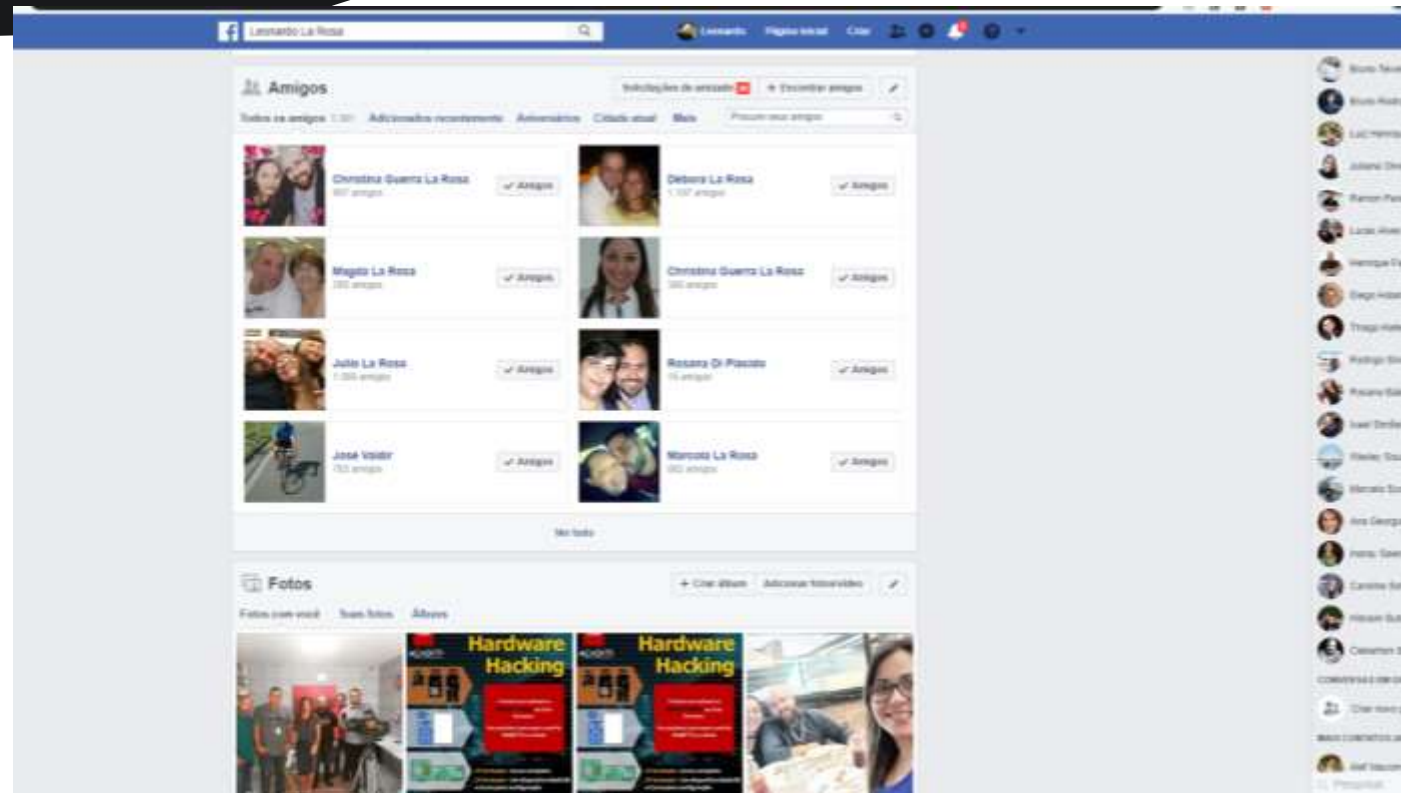
OSINT



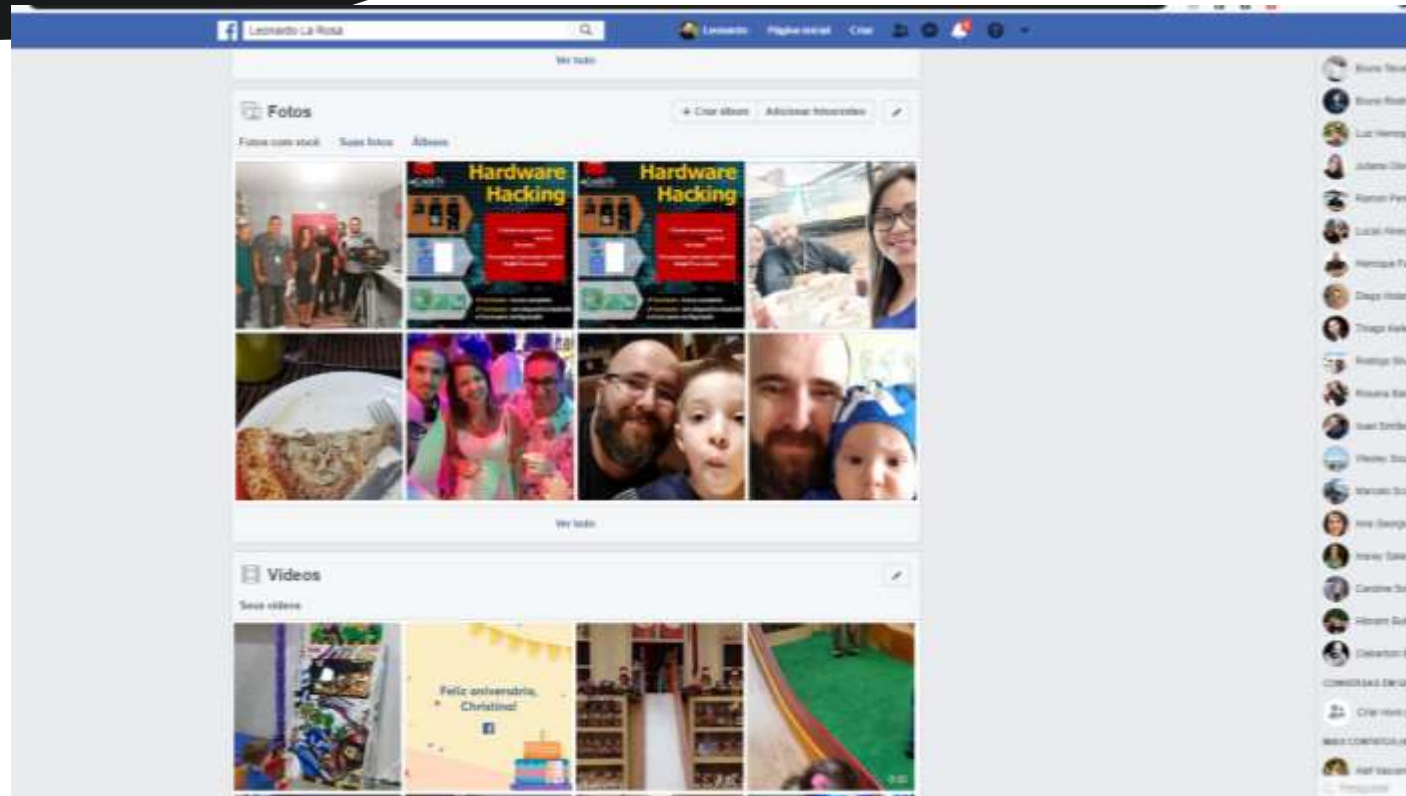
OSINT



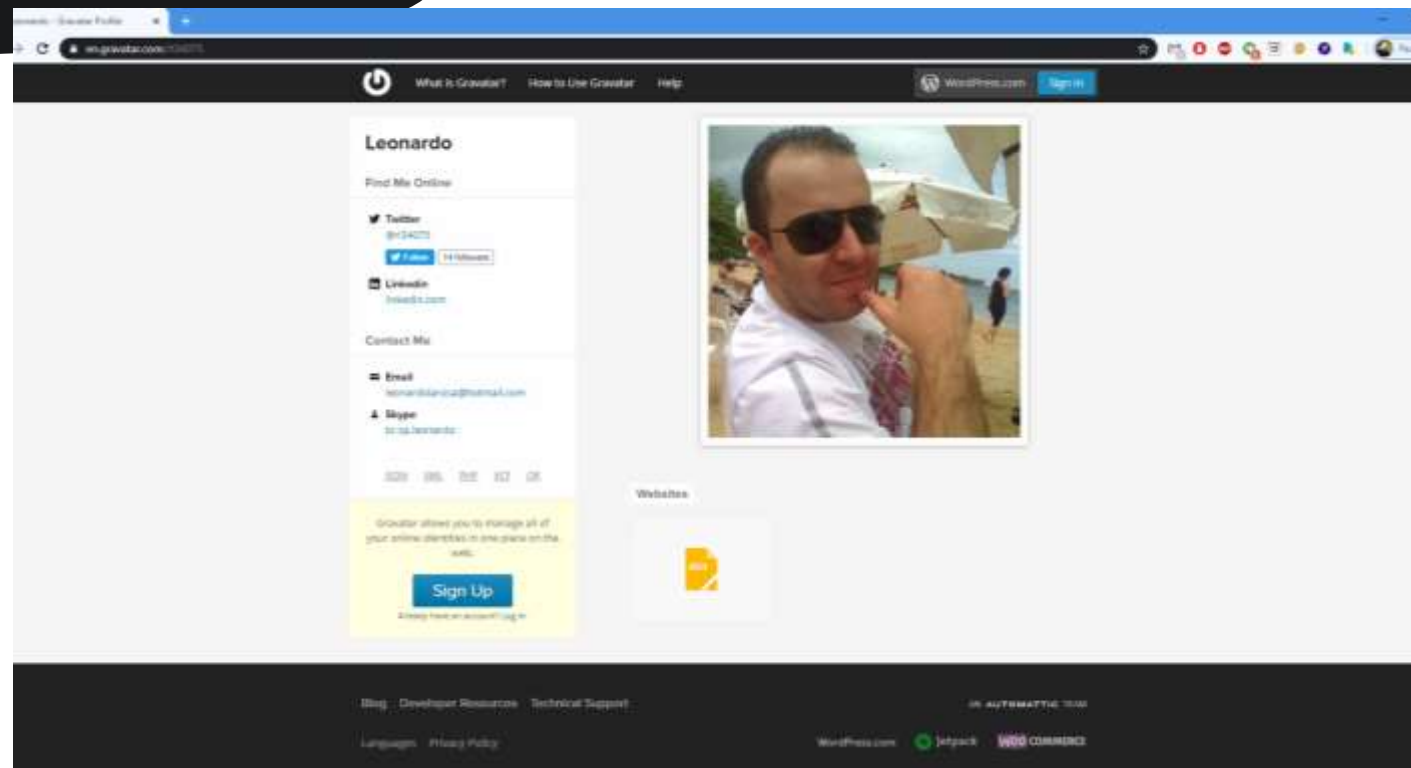
OSINT



OSINT



OSINT



OSINT



The screenshot shows a LinkedIn profile for Leonardo La Rosa. The profile includes a header with the LinkedIn logo, navigation tabs for 'Pessoas', 'Leonardo', and 'La Rosa', and buttons for 'Cadastrar-se' and 'Entrar'. The main profile section features a profile picture, a cover image, and the name 'Leonardo La Rosa' with his title 'Infrastructure & Cyber Security Manager - CSCU, NSF, CND, CEH, CEI' and location 'São Paulo, São Paulo, Brasil'. A blue button 'Entre para se conectar' is visible. To the right, a section titled 'As pessoas também viram' lists several other professionals. The 'Sobre' section contains a detailed bio in Portuguese, mentioning 15 years of experience in IT management and a focus on information security.

Leonardo La Rosa
Infrastructure & Cyber Security Manager - CSCU, NSF, CND, CEH, CEI
São Paulo, São Paulo, Brasil · + de 500 conexões

As pessoas também viram

- Claudio Dodt**
Especialista de Cibersegurança e Proteção de Dados, CISSP, CISM, CRISC, ISO27K LA, ITIL Expert | +22K
- Renata Della Villa Fata**
Consultora de Segurança da Informação
- Guilherme Benchinol**
CEO e Fundador da XP Inc.
- Amanda Balzano**
Analista Sênior de Security Awareness | EBANX
- Laios Barbosa**
Information Security Manager | CISSP | OSCP, OSWP, OSCP | SANS/GIACv18
- Jonathan Freitas**
Gerente de TI / Desenvolvimento de Sistemas / Metodologias Ágeis / Transformação Digital - ASP R, LITA R, PSM R, MSPQ R
- Eder CISSP**
CEH, CHFI, ECSA, OSCP, OSWRGCF, A, GPEN
Chief Operation Officer and Cyber Security in Brazilian Army
- Ana Catarina**
Public Security Analyst | ISO 27001

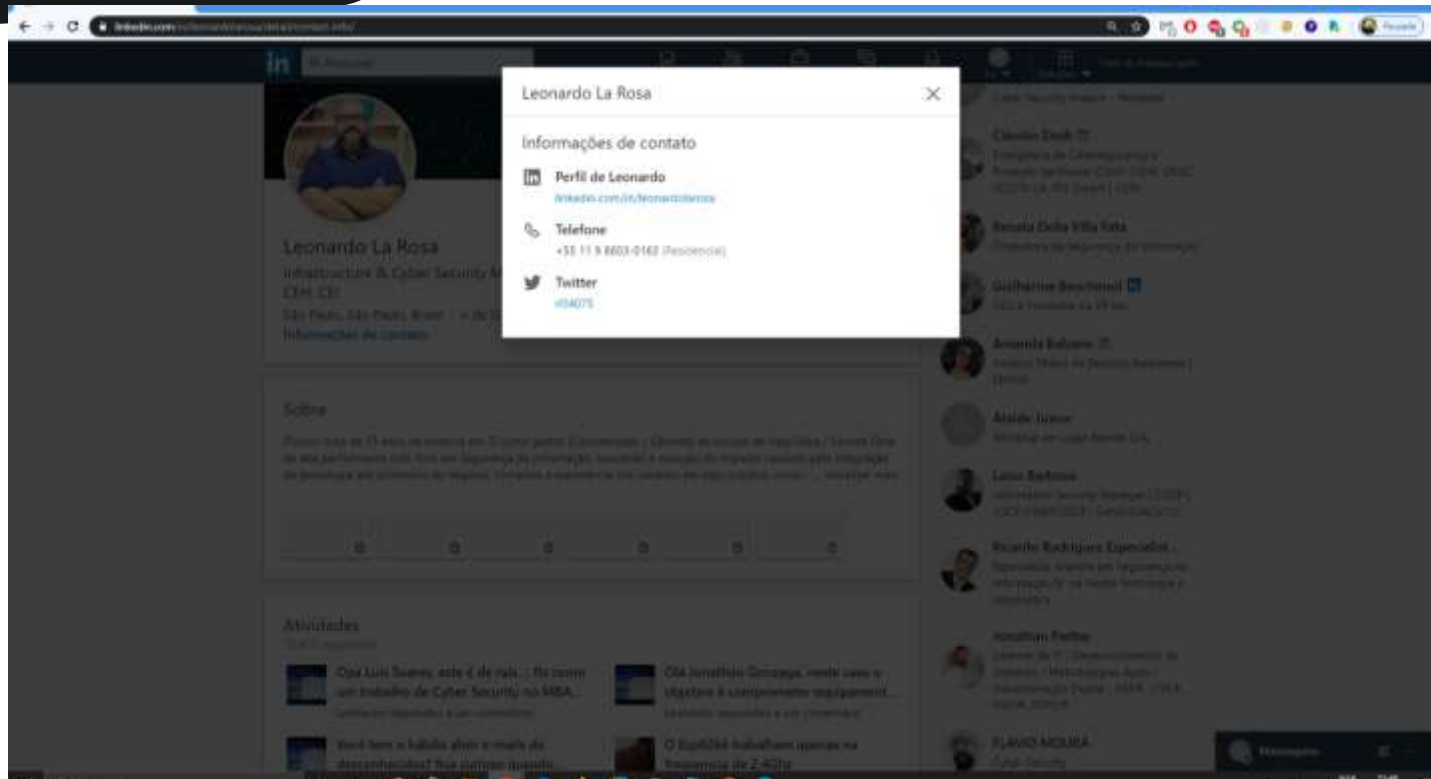
Sobre

Possuo mais de 15 anos de vivência em TI como gestor (Coordenador / Gerente) de equipe de Help Desk / Service Desk de alta performance com foco em Segurança da Informação, buscando a redução do impacto causado pela integração da tecnologia aos processos do negócio, tomando a experiência dos usuários em algo positivo, comprovado em pesquisa de satisfação e entregas de Níveis de Serviço.

Dentre algumas entregas, seguem:

- Documentação de processos e implantação de Base de Conhecimento;
- Aumento na aderência à pesquisa de satisfação, bem como no resultado da pesquisa;
- Controle dos KPIs de fornecedores e aumento nos SLAs acordados;
- Integração do atendimento de TI a temas de negócio, convertendo o Service Desk em Central de Suporte Comercial.

OSINT



OSINT



Nome
Completo

Empresa
Atual

Empresa
Anterior

Conjuge e
Filhos

Fotos

Videos

Teams

E-mail

Telefone

Quais os impactos quando um Executivo é vítima de ataque?



O que é Phishing?

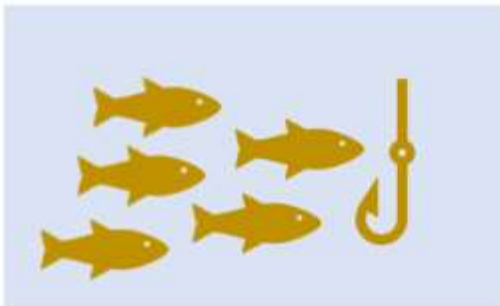


Phishing é uma maneira desonesta que **cibercriminosos usam para enganar** você para revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando e-mails falsos ou direcionando você a websites falsos.

Quais os impactos quando um Executivo é vítima de ataque?

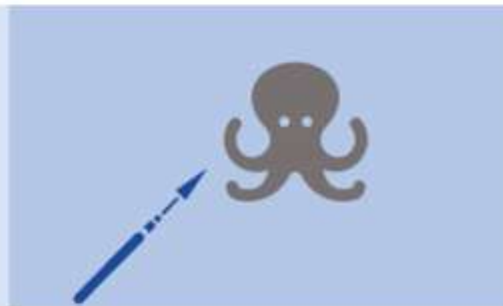


Tipos de Phishing



PHISHING EM ESCALA

Ataque onde os fraudadores lançam uma ampla rede de ataques que não são altamente visados



SPEAR PHISHING

Adaptado a uma vítima específica ou grupo de vítimas usando dados pessoais



WHALING

Tipo especializado de phishing que tem como alvo uma vítima "grande" dentro de uma empresa, como executivos.

Quais os impactos quando um Executivo é vítima de ataque?



Anatomia de um Phishing – acaditl.com.br



Para esta demonstração, realizaremos a Aquisição do Domínio: acaditl.com.br através do RegistroBR (<https://registro.br/>)



R\$ 40,00
por 1 ano

Ao escrever o domínio em caixa alta, teremos “ACADITL.com.br”, mesmo assim, o endereço “**acaditl.com.br**” poderia passar despercebido por alguns usuários desatentos.

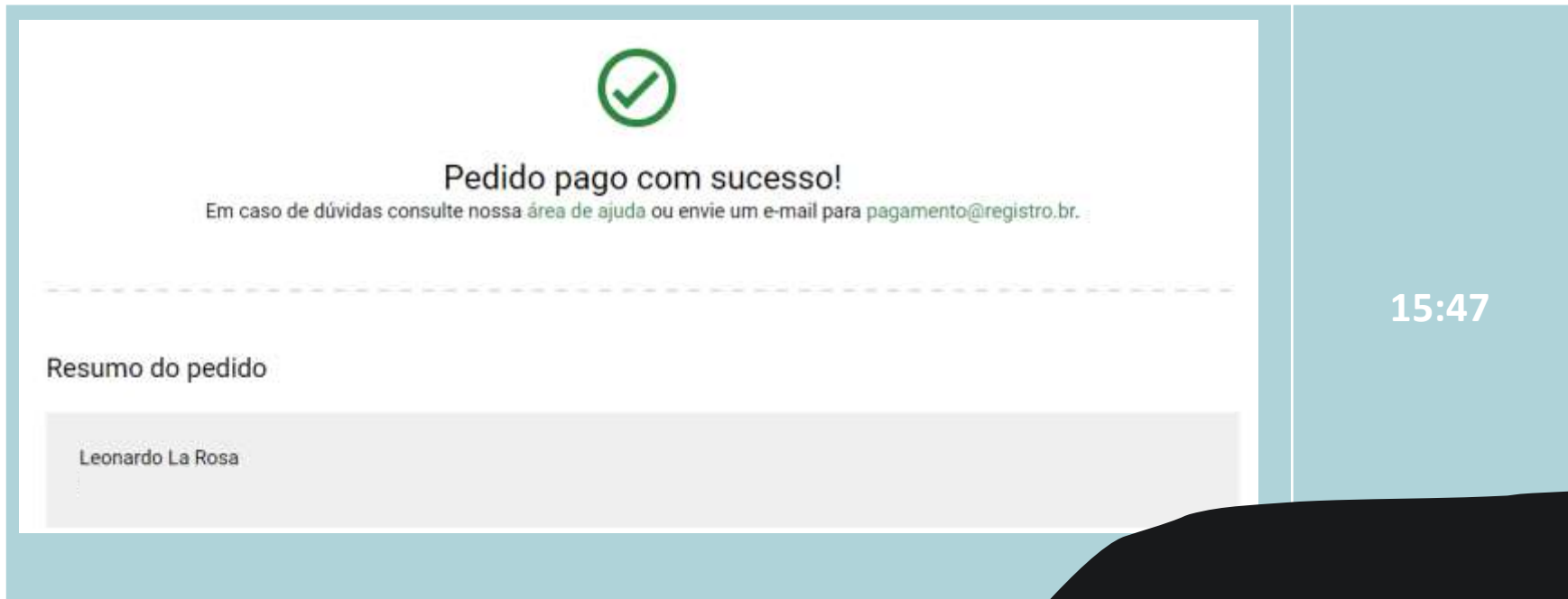
DOMÍNIO ↓	STATUS	EXPIRAÇÃO ↓	CONTATO
ACADITL.COM.BR	 Registrando		

15:45

Anatomia de um Phishing – e-mail



Às 15:47 o domínio já estava registrado em meu nome e disponível para utilização.



Anatomia de um Phishing – e-mail



Realizei a configuração em minha hospedagem e em alguns minutos o site já estava no ar.

Servidor 1
ns1046.hostgator.com.br

Servidor 2
ns1047.hostgator.com.br

ⓘ No momento, os servidores DNS do domínio se encontram em transição.
Servidores DNS externos poderão ser delegados em seu domínio em aproximadamente 1h59m45s

15:51

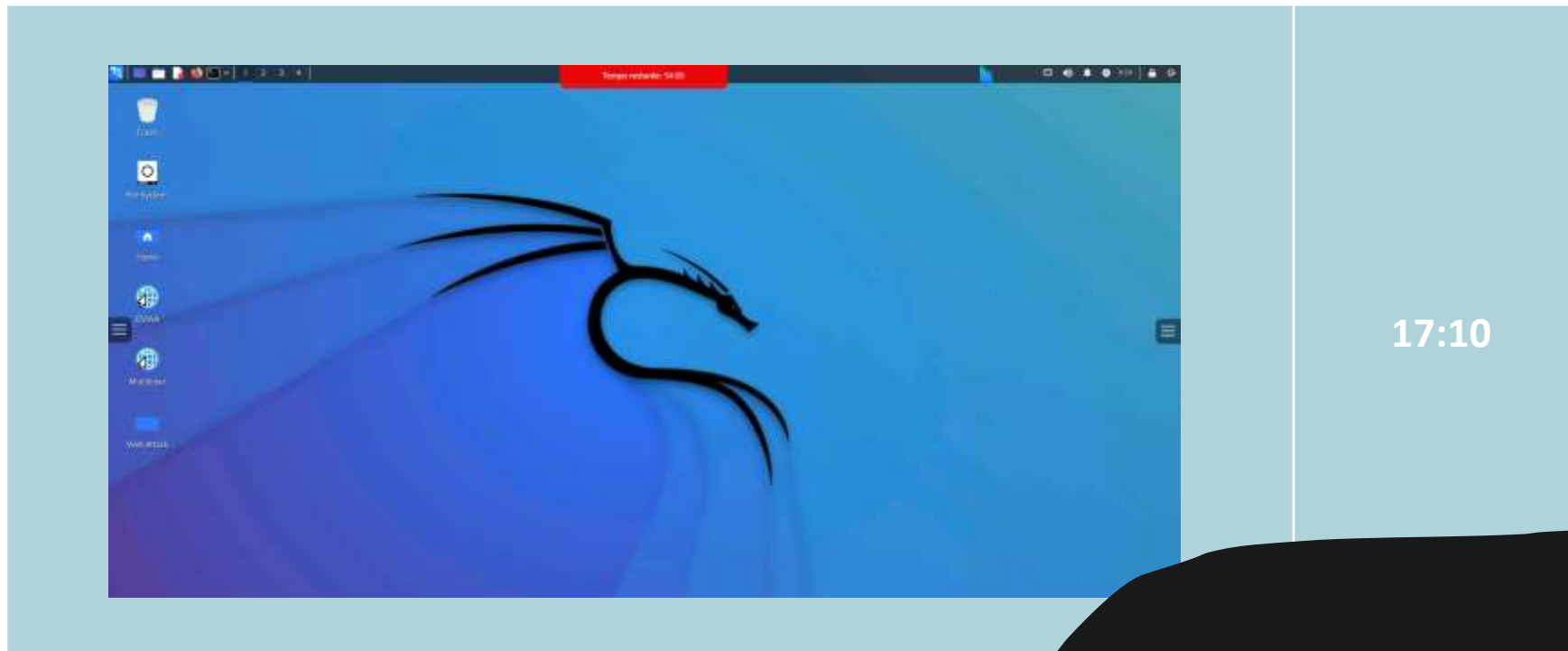


15:51

Anatomia de um Phishing – e-mail



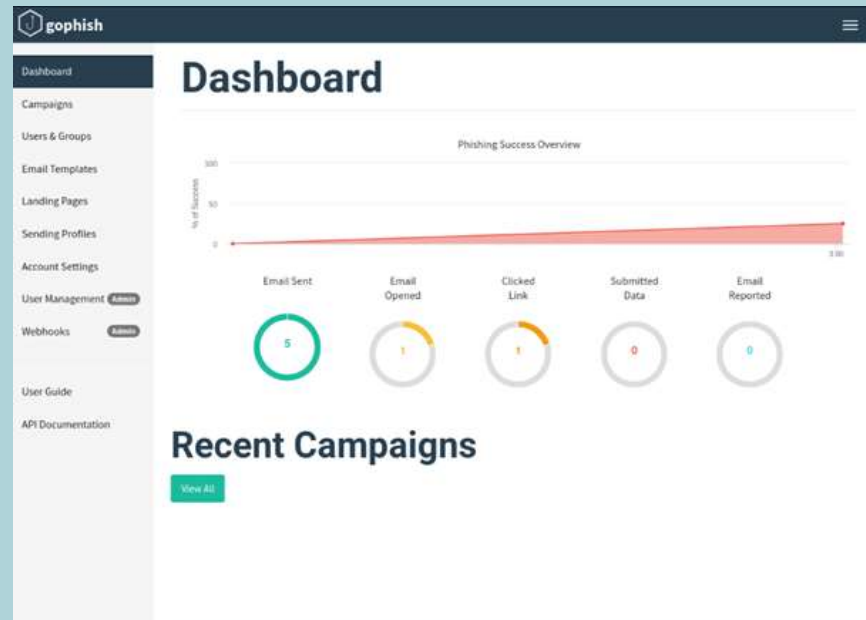
Às 17:10 meu servidor estava no ar, em um provedor em NY



Anatomia de um Phishing – e-mail



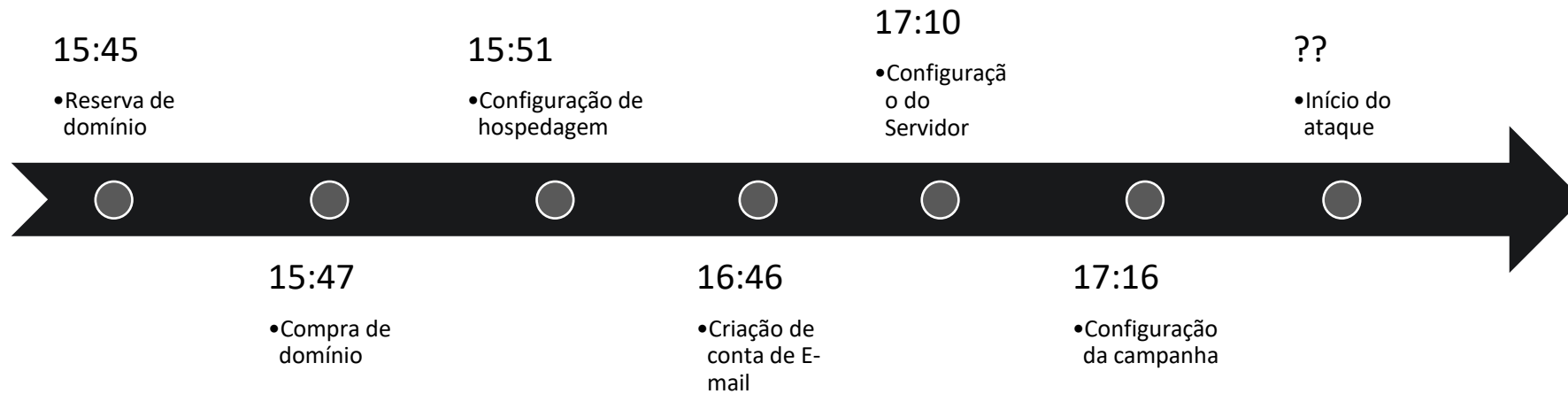
A partir daí basta criar a campanha de phishing e direcionar para os usuários



17:16

Anatomia de um Phishing – e-mail

Veja agora em uma linha do tempo



Em menos de 2h todo ambiente de phishing estava preparado e operando.

Anatomia de um Phishing – e-mail



Seu time de Segurança está preparado para estes ataques?

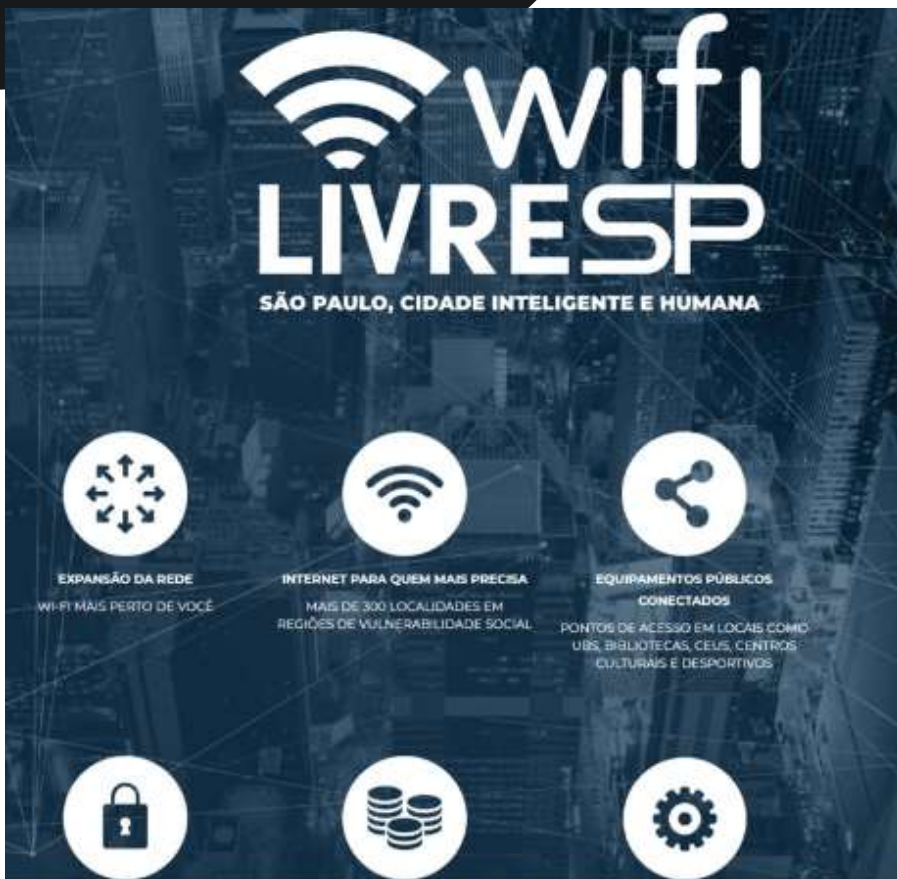
E o time de Segurança dos seus clients?

E o time de Segurança de seus parceiros e fornecedores?

Anatomia de um Phishing – Wi-Fi



Uso de WiFi Publico



Neste novo ataque de phishing abordaremos a questão do uso de WiFi aberto ou sem proteção.

Uso de WiFi Publico



Uso de WiFi Publico



Comportamento dos usuários



11% das organizações utilizam um segundo fator de autenticação

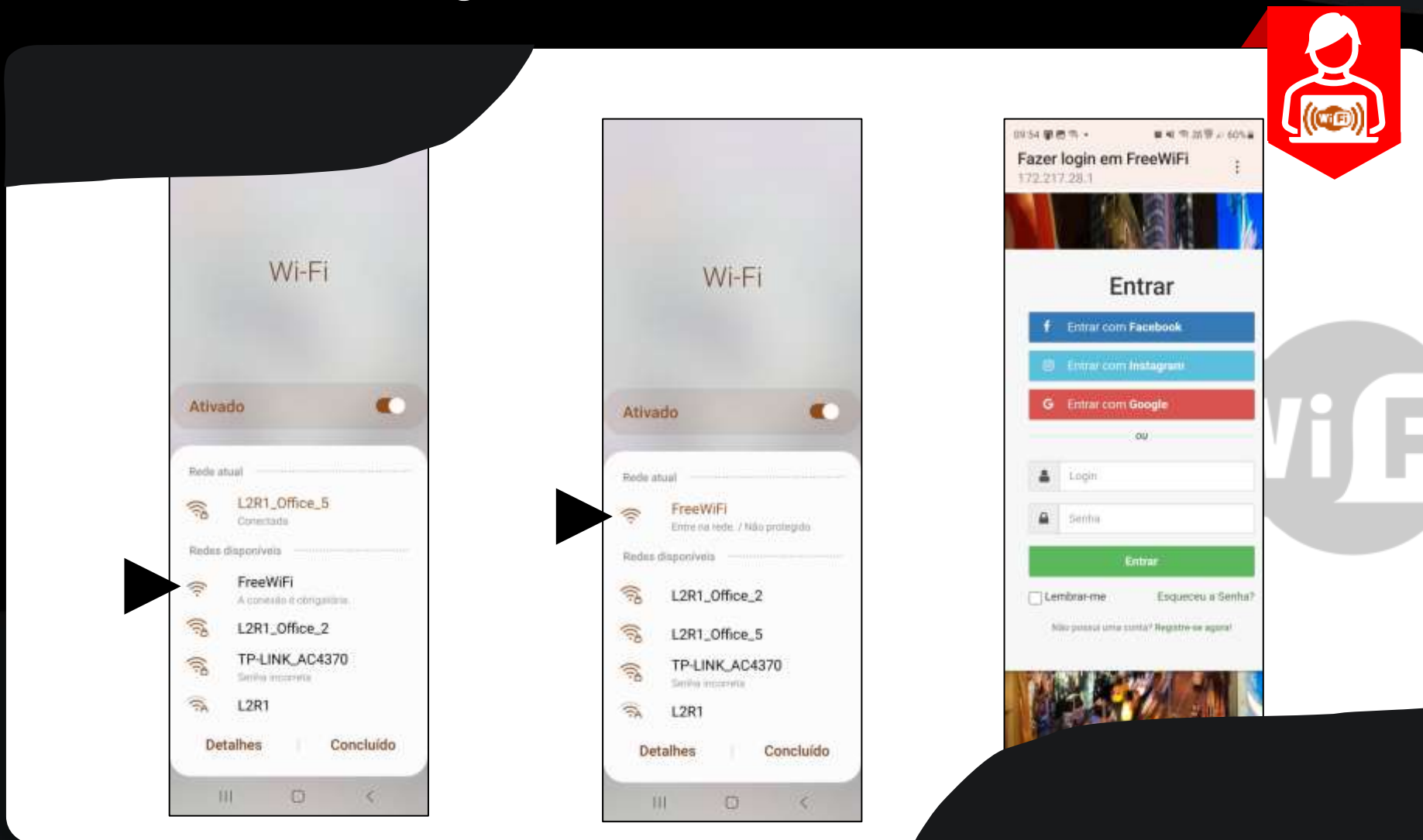


73% das contas online usam senhas duplicadas

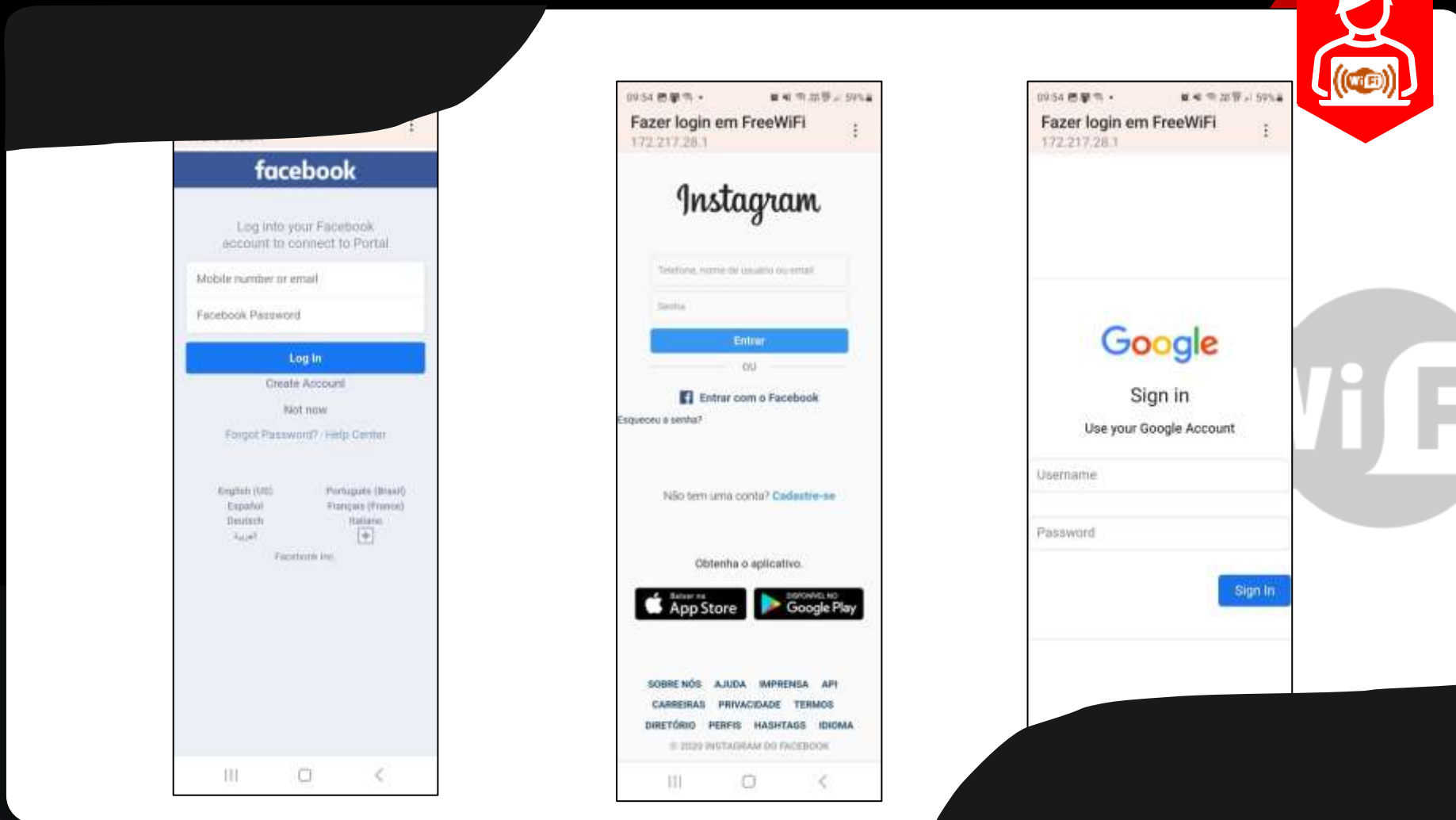


58% dos brasileiros acreditam que suas informações pessoais estão seguras ao acessar uma rede WiFi pública

Anatomia de um Phishing – Wi-Fi



Anatomia de um Phishing – Wi-Fi



Anatomia de um Phishing – Wi-Fi



WiFi Phishing Admin

SSID

Free_WiFi

FreeWiFi

MODELO

Portal.htm

Portal.htm
index.htm
facebook.htm
insta.htm
google.htm
email.htm

RETORNO

erro1.htm

erro1.htm
erro2.htm
erro3.htm
erro4.htm

DADOS

facebook: test@exemplo.com.br
instadados: 123456789

Salvar

Nome da
Rede

Modelo de
página

Retorno de
Erro

Dados
capturados

Gerenciamento por WiFi ou por USB



Como me protejo?



Não utilize WiFi aberto

Shoppings e restaurantes costumam oferecer serviços de internet gratuitos para seus clientes. Uma pessoa mal intencionada pode capturar os dados que estão passando pela rede



Utilize dados da operadora

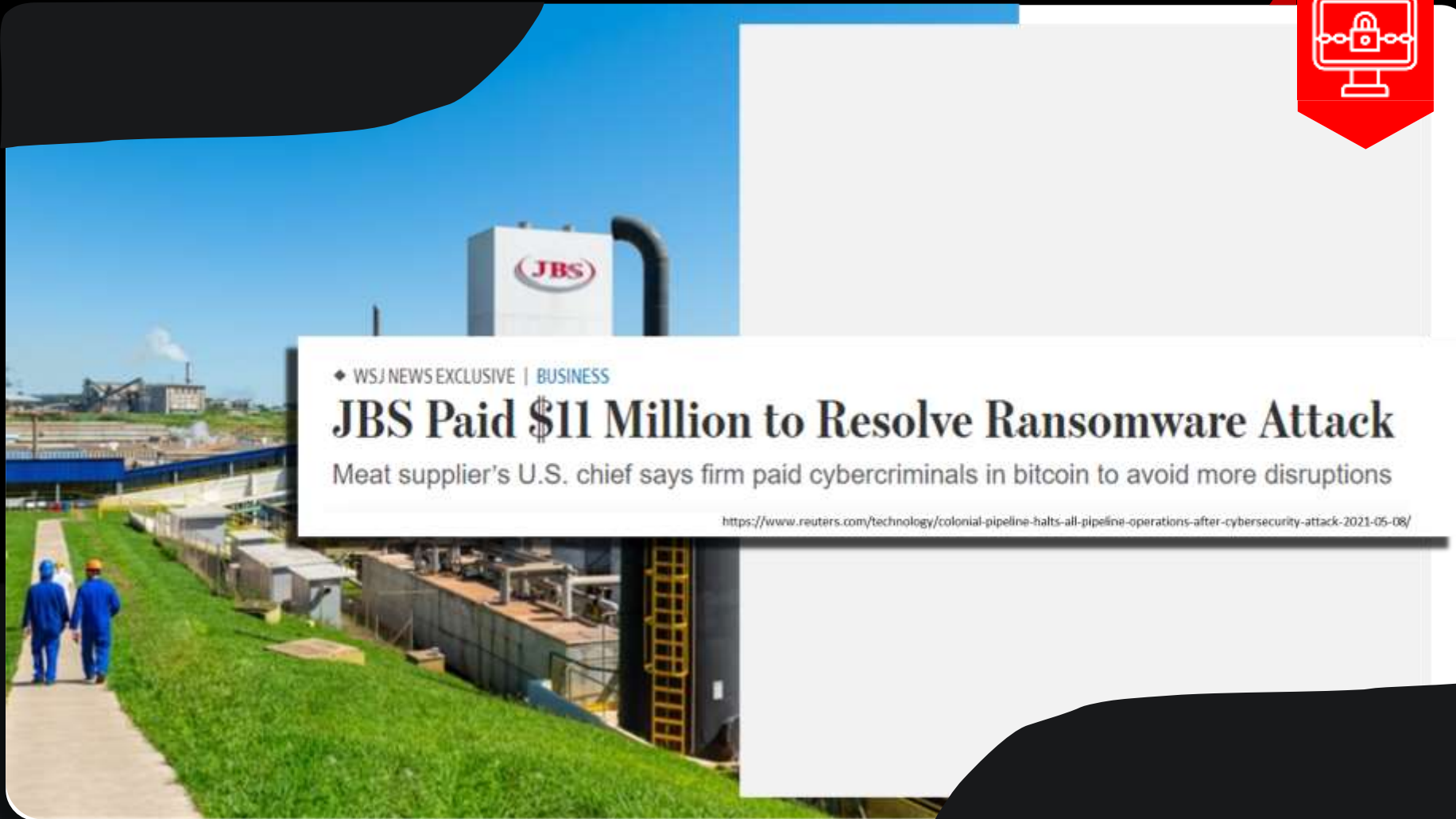
Sempre que possível, utilize os dados oferecidos pela operadora de telefonia. Caso precise utilizar WiFi aberto, utilize clientes de VPN para aumentar a sua segurança.

Ataques de Ransomware



**Qual o custo do seu negócio
indisponível por 24 horas?**

Ataques de Ransomware




Ataques de Ransomware



A Porto Seguro é a mais nova empresa brasileira a sofrer um ataque cibernético. A seguradora reportou nesta quinta-feira, 14/10, o ataque à Comissão de Valores Mobiliários, mas disse apenas que sofreu 'uma instabilidade parcial em seus canais de atendimento e alguns de seus sistemas'. Porém, a Porto Seguro não revelou a natureza do ataque - não diz se foi ransomware ou outra modalidade.

<https://www.convergenciadigital.com.br/Seguranca/Porto-Seguro-e-a-nova-vitima-de-ataque-cibernetico-58450.html?UserActiveTemplate=mobile>

Os ataques continuam ocorrendo



09/01

TOCANTINS GOVERNO DO ESTADO

Ataques miram setor de Governo, Tocantins é o alvo da vez

[Link](#)

Após incidente, sites governamentais do Tocantins são restabelecidos

[Link](#)

11/01

TRIBUNAL DE JUSTIÇA DO ESTADO DO PARÁ

Tribunal de Justiça do Pará sofre ataque cibernético

[Link](#)

JP

Canais da Jovem Pan no YouTube são alvos de invasão cibercriminosa

[Link](#)

06/01

MP AM MINISTÉRIO PÚBLICO DO ESTADO DO AMAPÁ

Ataque cibernético impacta sistema eletrônico do Ministério Público do Amazonas

[Link](#)

04/01

CÂMARA MUNICIPAL DE CURITIBA/PR

Incidente em terceiro impacta operação da Câmara Municipal de Curitiba

[Link](#)

CNJ

Cibercriminoso invade CNJ e publica falso mandado de prisão

Alexandre de Moraes

FONTE: <https://www.securityreport.com.br/email/InfoSR2023>

Os ataques continuam ocorrendo



Dados da Cybersecurity Ventures apontam que os danos causados por crimes cibernéticos devem chegar a US\$ 8 trilhões ainda em 2023 – valor que coloca o **crime cibernético como terceira maior economia do mundo depois dos EUA e da China**

<https://itforum.com.br/noticias/os-desafios-da-seguranca-cibernetica-em-2023-e-nos-proximos-anos/>

Protegendo o Ambiente



**Como a Segurança da
Informação pode ajudar a
proteger minha empresa?**

Protegendo o Ambiente



A Segurança da Informação apoia o negócio implementando controles:



Preventivo

Controles de Segurança como Firewall, AntiSpam criam uma barreira para evitar ataques.



Detectivo

Caso algum dos controles Preventivos falhe, é importante que os ataques sejam detectados o quanto antes.



Reativo

Uma vez detectada a ameaça, inicia-se o processo de contenção e recuperação dos danos.

Protegendo o Ambiente



**Além dos controles sistêmicos,
os funcionários também devem
ficar atentos a:**



E-mails

Não abra e-mails de origem desconhecida e sempre desconfie de links e anexos de e-mails de fora da organização.



Fraudes

Os bancos nunca solicitam senhas ou dados de cartões aos seus clientes, portanto, cuidado com e-mails com este conteúdo.



Privacidade

Evite compartilhar dados pessoais em planilhas e emails.

Protegendo o Ambiente



Uso dos recursos de tecnologia

Não utilize e-mails e acessos corporativos para uso pessoal.



Dispositivos

Não conecte dispositivos desconhecidos ao seu computador.



Navegação

Tenha hábitos saudáveis de navegação na Internet.

CULTSEC

A NOVA ERA DA CONSCIENTIZAÇÃO



Siga-nos nas redes sociais



/school/acaditi



/academiainovadora



/acaditi_oficial



/@ACADITI