FÁBRICA
de programadores

3 DE JULHO DE 2024
FORTALEZA – CEARÁ

#3

# SEGURANÇA NA ERA CIBER

## CONHEÇA OS RISCOS, OS DESAFIOS E AS ESTRATÉGIAS PARA SE ATUALIZAR E SE PROTEGER NA WEB

JOÃO FILHO TAVARES

Jony do Vale é veterano em segurança da informação e vive no dia a dia o desafio de garantir a cibersegurança em negócios

## EXPEDIENTE

**EXPEDIENTE FUNDAÇÃO DEMÓCRITO ROCHA**
Presidente Luciana Dummar | Diretor Administrativo-Financeiro: André Avelino de Azevedo | Gerente-Geral: Marcos Tardin | Gerente Editorial: Lia Leite | Gerente de Marketing e Design: Andréa Araújo | Designers: Kamilla Damasceno e Welton Travassos | Gerente de Audiovisual: Chico Marinho | Gerente de Projetos: Raymundo Netto | Analistas de Projetos: Aurelino Freitas e Fabrícia Góis | Analista de Contas: Narcez Bessa

**UNIVERSIDADE ABERTA DO NORDESTE (Uane)**
Gerente Educacional: Prof. Dr. Deglaucy Jorge Teixeira | Coordenadora Pedagógica: Profª Ms. Jôsy Braga Cavalcante | Coordenadora de Cursos: Esp. Marisa Ferreira | Secretária Escolar: Márcia Doudement | Desenvolvedora Front-End: Isabela Marques | Estagiários(as) em Mídias e Tecnologias para Educação: Ágata Ribeiro e Alisson Aragão | Estagiários(as): Bianka Silva, Lucas Gomes Gonçalves, Wesley Militão Fernandes Mendes, Marcio Renan de Souza Gonçalves

**FÁBRICA DE PROGRAMADORES**
Concepção e Coordenação Geral: Hamilton Nogueira e Valéria Xavier | Coordenação de Conteúdo: Viviane de Menezes | Analista de Operações: Alexandra Carvalho | Analista de Projetos: Hérica Paula Morais | Editora de conteúdo do caderno: Paula Lima | Textos: Letícia do Vale e Lucas Casemiro | Design: Natasha Ellen

**PATROCÍNIO**
ALECE ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ

**REALIZAÇÃO**
FUNDAÇÃO DEMÓCRITO ROCHA

## ESTE É O CADERNO #3

O Fábrica de Programadores é um projeto que se propõe a capacitar cerca de 2.000 jovens por ciclo. A motivação da edição de 2024 é que cada um saiba fazer seu próprio game. Esta já é a terceira edição do projeto que alcança gratuitamente jovens e profissionais de tecnologia em todo o País.

Hoje, publicamos o terceiro caderno de uma série de quatro que tem como objetivo ampliar o olhar sobre as oportunidades da tecnologia, os debates e reflexões necessários em um universo que se desenha ainda novo em muitos aspectos.

O assunto que norteia os debates desta edição é a segurança cibernética. Quem de nós já não foi vítima de alguma abordagem de hackers? E sorte de quem não caiu nas armadilhas cibernéticas. Nas páginas a seguir, apresentamos os desafios de empresas e pessoas físicas em driblar a ação de golpistas e cibercriminosos. O que é válido para toda empresa e para todo usuário de internet é desenvolver um senso crítico mais aguçado, desconfiar de promessas com ganhos muito valiosos e evitar clicar em qualquer link, por exemplo.

Boa leitura!




## ÍNDICE

# CIBERSEGURANÇA:

## DESAFIOS E MEDIDAS NA ERA DIGITAL

**ATAQUES CIBERNÉTICOS CAUSAM PREJUÍZOS A PESSOAS E ORGANIZAÇÕES. AVANÇO DA TECNOLOGIA E DEPENDÊNCIA DE SISTEMAS DIGITAIS PROVOCAM SOFISTICAÇÃO DE AMEAÇAS**

**Lucas Casemiro**
**lucas.casemiro@opovo.com.br**

Jony do Vale é head de TI e Segurança da Informação da empresa cearense Wiser Tecnologia

A tecnologia já é parte indissociável da vida humana, e praticamente todos os tipos de serviço dependem, de algum modo, da Internet. Não é errado afirmar que as ameaças a soluções tecnológicas tornam todos, em algum nível, vulneráveis. Como nos filmes de ficção científica, os impactos de um ataque cibernético podem ocasionar caos à medida em que têm potencial para afetar gravemente o funcionamento da sociedade, causando prejuízos incalculáveis a pessoas, empresas e governos. É nesse contexto que a cibersegurança tornou-se uma preocupação crescente para organizações e indivíduos no mundo todo.

A segurança cibernética é definida como a área da computação que foca na proteção de sistemas e comunicação de dados contra ameaças como vírus e hackers. Também chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas, as práticas de segurança cibernética dizem sobre a proteção contra ataques maliciosos a hardwares e servidores, computadores pessoais e dispositivos móveis, redes e dados.

Se você vive no Brasil, os riscos de sofrer tentativas de ataques cibernéticos são ainda maiores. Isso porque o País é o segundo mais atacado por hackers no mundo, atrás apenas dos Estados Unidos, e continua sendo o principal alvo de ataques na América Latina, de acordo com o Relatório de Inteligência de Ameaças da líder global de cibersegurança NetScout, divulgado no segundo trimestre deste ano. Apenas no segundo semestre do ano passado, o Brasil sofreu 357.422 ataques, um aumento de 8,86% quando comparado com o primeiro semestre do mesmo ano, quando 328.326 investidas foram registradas.

Existe uma explicação para o Brasil estar no topo desse ranking. A globalização e o aumento do trabalho remoto, acelerados pela pandemia, trouxeram novos desafios para a cibersegurança. Nos últimos anos, empresas precisaram se adaptar para expandir sua atuação online, e entrar em novos espaços aumentou a vulnerabilidade das corporações. Exemplo disso é o trabalho remoto, que veio para ficar.

"A pandemia provocou o aumento do trabalho em casa, o que criou um desafio para as empresas. Em um computador na empresa podemos retirar as portas USB, impedir que um usuário instale um programa, etc. Mas quando a pessoa usa seu computador pessoal?", questiona Marcial Fernández, professor na graduação e no Programa de Pós-graduação em Ciência da Computação da Universidade Estadual do Ceará (Uece) e consultor do Governo do Estado do Ceará na área de Tecnologia da Informação e Comunicação (TIC).

No home office, a incapacidade de controlar diretamente os dispositivos pessoais dos funcionários aumenta a vulnerabilidade da empresa, exigindo dela políticas mais rigorosas para garantir a segurança de dados e sistemas utilizados fora do ambiente corporativo, como uso de VPNs e reforço na educação dos colaboradores sobre os riscos e medidas de proteção.

"O problema de uma empresa pequena é que não tem muitos recursos para se proteger, seja para compra de equipamento ou serviço, seja para contratar ou treinar pessoal. Mas os prejuízos também podem ser enormes. Só o fato de se preocupar com segurança desde o início, desenvolvendo um software, pode melhorar e mitigar os danos. Da mesma forma que uma empresa precisa se preocupar com a qualidade dos produtos e serviços, também precisa se preocupar com a qualidade das ferramentas que utiliza", afirma o professor Marcial Fernández.

### TOP 3 SETORES MAIS ATINGIDOS POR ATAQUES HACKERS NO BRASIL

*no período de jul-dez de 2023*

1. Telecomunicação sem fio - 82.065 ataques (+142.47% em relação ao primeiro semestre de 2023)
2. Transporte de cargas - 25.620 ataques
3. Processamento de dados - 25.130 ataques

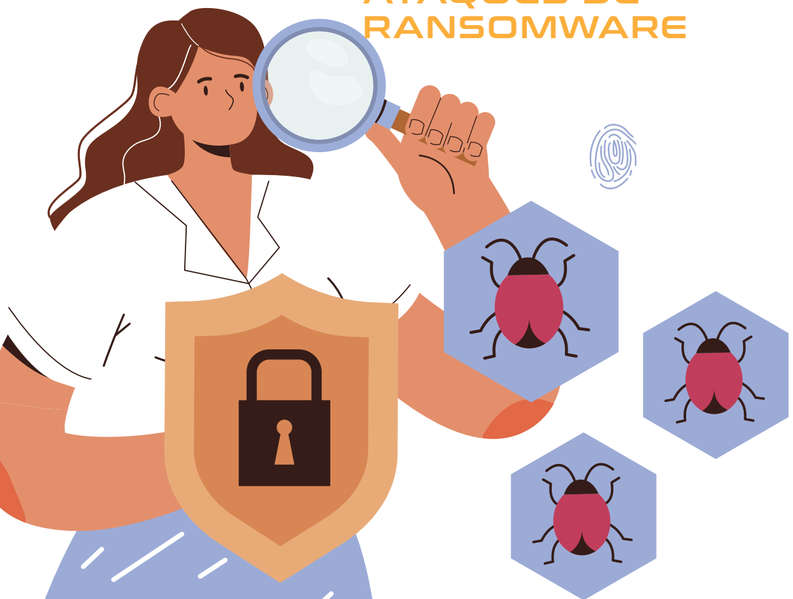
**Fonte:** Relatório de Inteligência de Ameaças. NetScout, 2024

## COMBATENDO ATAQUES NA PRÁTICA

Jony do Vale, um veterano com mais de 20 anos de experiência em infraestrutura, segurança da informação e gestão de pessoas, vive no dia a dia o desafio de garantir a cibersegurança em negócios. Como head de TI e Segurança da Informação da empresa cearense Wiser Tecnologia, fundada em 2019, ele relata que os problemas mais comuns na área incluem principalmente ataques de ransomware, uma espécie de vírus que sequestra informações e exige recompensa para liberar o sistema.

"O que geralmente acontece? O sistema para, alguma coisa deixa de funcionar e quando ela (a empresa) vai verificar, os arquivos estão criptografados e tem um arquivo de texto informando se os arquivos foram sequestrados, estão criptografados com um código forte, e (os atacantes) pedem um resgate, um determinado valor em bitcoin em uma determinada conta", relata.

> OS PROBLEMAS MAIS COMUNS NA ÁREA INCLUEM PRINCIPALMENTE ATAQUES DE RANSOMWARE



É na hora que o sistema da empresa para de funcionar que a Wise costuma ser acionada. "Eles (empresas clientes) identificam qual foi a máquina ou as máquinas infectadas. A gente consegue, por dentro do próprio sistema de antivírus, isolar essa máquina do parque. A máquina já não tem mais comunicação com a rede interna, ela fica em quarentena, na verdade. A gente isola para evitar a infecção das demais", explica. Nessa hora, ganha quem mantém backups atualizados. A restauração dos dados da empresa é feita em um outro disco, em uma máquina que não esteja infectada.

Além da atuação combativa, uma das linhas de atuação contra ciberataques é a boa e velha informação. Para isso, existem serviços preventivos de conscientização dos usuários. Nesse sentido, a estratégia é desenvolver nas pessoas um senso crítico mais aguçado, instruindo-as a desconfiar de promessas com ganhos muito valiosos e evitar clicar em qualquer link, por exemplo.

"Ninguém está ileso. Hoje em dia, todo mundo é vulnerável de receber um phishing, um malware, e ter ou os dados coletados ou sofrer alguma fraude de cartão, através de um phishing, e as empresas também", frisa Jony do Vale.



**Empresa cearense Wiser Tecnologia, fundada em 2019, promove soluções tecnológicas para outros negócios**

## UMA FACA DE DOIS GUMES

O avanço da tecnologia, aliado ao aumento da dependência de sistemas digitais, fez com que organizações e indivíduos contem com mais recursos para se proteger na rede. "Assim como a maior parte das novas soluções de computação que são criadas atualmente, a inteligência artificial tem sido a base para a criação de novas soluções que sejam mais robustas e automatizadas, possibilitando assim uma resposta a incidentes mais ágil. Além de IA, blockchain tem sido usada para aumentar a segurança de transações e dados, proporcionando uma camada adicional de proteção contra adulteração de dados", lembra Rafael Lopes, coordenador do Programa de Pós-graduação em Ciência da Computação da Uece.

Ao passo que facilitam o combate a ataques cibernéticos, esse cenário também fez com que as ameaças cibernéticas acompanhassem o desenvolvimento de outras áreas, gerando uma sofisticação dos ataques. A utilização de IA per si já não é mais garantia de segurança, uma vez que invasores também utilizam a tecnologia para auxiliar os ataques.

"O uso das LLMs (modelos de linguagem ampla), como ChatGPT, Gemini e CoPilot, tem facilitado para os atacantes. Veja um exemplo: a maioria das pessoas cria uma senha usando dados pessoais, aniversário, nome do cachorro, nome da escola que estudou, cidade em que passa as férias. Um LLM pode combinar essas informações pesquisadas nas redes sociais e descobrir a senha", explica Marcial Fernández, professor de Ciência da Computação.

"O que acontece na área de segurança da informação é que ferramentas que são construídas para trazer uma melhoria de vida, de trabalho, de formas de se fazer algo, são utilizadas também para o mal. Hoje, com inteligência artificial, você percebe isso claramente. Teve uma época que se utilizava sistemas, softwares, para invadir. Só que esses softwares tinham que ser configurados e precisava de que um profissional inserisse comandos para acontecer. Hoje, um bot configurado consegue dar milhões de comandos de uma vez só e tentar isso várias e várias vezes", informa Wandson Alves, analista de infraestrutura de TI com mais de 12 anos de atuação na área da Tecnologia da Informação.

Apesar do avanço tecnológico, o especialista diz haver vários registros de invasões envolvendo roubo de informação que não utilizam tecnologia complexa. "Um hacker lá fora entra em contato telefônico com uma pessoa da empresa, um recepcionista, se passa por um grande gestor dentro da empresa e consegue, através de um protocolo de argumentações, informações importantíssimas sem utilizar um código", exemplifica.

Isso denota que o fator humano é essencial para a segurança da informação. "Há um despreparo muito grande quando se trata de empresa e de segurança da informação, principalmente se tratando do Ceará. Vários gestores colocam a responsabilidade da segurança da informação e da privacidade de dados como um ponto intrínseco da TI, como responsabilidade íntima da TI, e na verdade não é só TI, apesar de todos os dados estarem sendo direcionados para o setor de TI", relata Wandson.

Nesse sentido, as políticas de governança corporativa garantem que as empresas implementem medidas adequadas e permaneçam em conformidade com regulamentações legais e industriais, complementa o professor Rafael Lopes. "Essas políticas desempenham um papel crucial na segurança cibernética, estabelecendo normas e práticas obrigatórias que as organizações devem seguir para proteger suas informações", exemplifica o professor.

## GOVERNOS AMEAÇADOS

Relembre casos de ataques hackers a órgãos governamentais no Brasil nos últimos anos:

**> Em 2021,** os sites do Sistema Único de Saúde (SUS), Conecte SUS (aplicativo do Ministério da Saúde responsável pelos dados de vacinação dos brasileiros), Polícia Rodoviária Federal, Ministério da Economia, Controladoria Geral da União (CGU) e Instituto Federal do Paraná sofreram uma série de ataques. Os criminosos exigiram uma determinada quantia para o restabelecimento das informações e a devolução dos acessos.

**> Em 2022,** páginas online do Governo do Ceará sofreram ataques hackers. Durante a ação, os invasores veicularam frases xenofóbicas contra nordestinos, apoio golpista e contestação aos votos a favor de Lula, na época o presidente eleito. O Governo conseguiu contornar as investidas no dia seguinte. Os ataques foram assinados pelo grupo "KillSec Team", também autor da invasão à Secretaria da Fazenda (Sefaz) de Alagoas.

**> Em 2023,** o datacenter da Secretaria de Educação e Esportes de Pernambuco sofreu invasão que comprometeu os dados e processos da pasta, afetando o edital de seleção de gestores de um órgão vinculado à pasta.



## COMO SE TORNAR UM PROFISSIONAL DE CIBERSEGURANÇA

A área de cibersegurança está em alta demanda, com diversas oportunidades para profissionais qualificados. Se você tem interesse em seguir essa carreira, aqui estão cinco passos que você pode seguir:

**1. Desenvolva as habilidades necessárias:**
> Conhecimento de sistemas operacionais, redes e protocolos de segurança
> Experiência com criptografia, análise de vulnerabilidades e testes de penetração
> Habilidade em programação e scripting

**2. Obtenha Educação: Diplomas**
> Graduação em Cibersegurança, Ciência da Computação, Engenharia da Computação ou áreas relacionadas
> Cursos técnicos em Segurança da Informação
**Certificações**
> CompTIA Security+
> Certified Ethical Hacker (CEH)
> CISSP (Certified Information Systems Security Professional)

**3. Ganhe Experiência Prática: Estágios e trabalhos de entrada**
> Procure oportunidades para aplicar seus conhecimentos e habilidades em um ambiente profissional. Voluntarie-se em projetos de segurança cibernética para ganhar experiência prática
**Participe de Competições e Desafios**
> Capture the Flag (CTF) e outros eventos de hacking éticos podem aprimorar suas habilidades e conhecimentos

**4. Construa seu Portfólio:**
> Documente seus projetos e experiências em segurança cibernética para demonstrar suas habilidades aos empregadores em potencial

**5. Construa sua rede**
> Participe de Comunidades Online de Segurança Cibernética
> Participe de Meetups e Eventos Locais
> Encontre um mentor experiente

CONHEÇA AS PRINCIPAIS PRÁTICAS EM SEGURANÇA

# CIBERNÉTICA

## ATAQUES PODEM CAUSAR PREJUÍZOS DIRETOS E A TERCEIROS

**Letícia do Vale**
**leticiavale@opovodigital.com**

À medida que crescem os usuários das ferramentas online, crescem, também, os riscos. Em uma realidade em que a internet tem tido um papel fundamental na comunicação entre indivíduos e empresas, as ameaças cibernéticas não podem ser subestimadas.

Além de danos pessoais e financeiros diretos, esses ataques também podem causar um 'efeito dominó' de prejuízos. É o que explica o consultor em cibersegurança, Ismael Júnior.

"Se a sua conta do Instagram, por exemplo, for roubada, os criminosos vão usar o seu networking e a sua credibilidade para vender alguma coisa falsa, e o prejuízo acaba tendo uma amplitude muito maior", indica.

Nesse sentido, confira dicas para evitar golpes cibernéticos no campo individual e empresarial.

## SEGURANÇA PARA INDIVÍDUOS

### FIQUE ATENTO ÀS PROPAGANDAS

Diariamente, usuários de redes sociais como Instagram, WhatsApp e Linkedin recebem uma enxurrada de propagandas com ofertas e facilidades até inacreditáveis. No entanto, não se deixe enganar por promessas tentadoras. Antes de clicar em qualquer link, é fundamental checar a validade desse endereço. Se o anúncio utilizar alguma marca conhecida, vá até o site oficial e verifique se a oferta realmente existe.

### INVISTA EM CAMADAS DE PROTEÇÃO

Tanto no computador quanto no celular, é importante manter os sistemas operacionais sempre atualizados. Além disso, o uso de um bom antivírus não pode ser dispensado. Assim, caso algum link ou arquivo malicioso passe despercebido, o sistema será capaz de alertá-lo.

### ATENÇÃO AO REMETENTE

Evite abrir e-mails de remetentes desconhecidos, principalmente se as mensagens indicarem algum tipo de oferta imperdível.

### NADA DE REPETIR INFORMAÇÕES

Use uma senha forte e diferente para cada rede social e demais logins. Outra medida relevante é ativar o segundo fator de autenticação, ou autenticação em duas etapas. Atualmente, a tática já está disponível nas redes sociais, em sites mais populares e funciona como mais uma barreira contra invasões e roubos de dados, já que exige um segundo método de identificação do usuário para o acesso pleno do sistema. As medidas são fundamentais já que é comum que os atacantes, ao descobrirem o login e a senha para uma determinada rede social, testem as mesmas informações em outras plataformas.

### DE OLHO NO CÓDIGO DE ÁREA

As tentativas de golpe não estão restritas a criminosos brasileiros. Quando as plataformas sofrem com vazamentos de dados, hackers do mundo inteiro ganham acesso a essas informações. Por isso, uma dica para identificar contatos suspeitos é ficar de olho no código de área de números desconhecidos. Se o contato não começar com +55, desconfie.

## SEGURANÇA PARA EMPRESAS

### COMECE DO BÁSICO

Como as empresas são feitas por pessoas, muitos ataques cibernéticos começam de forma semelhante aos direcionados para pessoas físicas. Assim, todos os cuidados básicos permanecem válidos, como ter senhas fortes, investir em antivírus, manter os sistemas operacionais dos computadores atualizados e orientar a equipe sobre ficar alerta a links e arquivos suspeitos. Além disso, é interessante que os programas utilizados nas empresas, como os do Pacote Office, sejam originais, ao invés de "crackeados".

### ATAQUES PODEM SER MAIS COMPLEXOS

Por vezes, os atacantes utilizam estratégias mais sofisticadas para golpear empresas, como sites e identidades falsos bem elaborados. Eles podem se passar por clientes ou até empresas parceiras em tentativas de negociações ou procura por dados. Nesse cenário, toda a equipe deve estar bem treinada para reconhecer essas situações e checar qualquer operação suspeita.

### ENTENDA O NÍVEL DE MATURIDADE E EXPOSIÇÃO DA SUA EMPRESA

Empresas de tamanhos diferentes têm necessidades diferentes. Por isso, antes de ter gastos com ferramentas tecnológicas modernas e uma equipe de T.I completa é interessante conhecer a fundo a realidade da empresa. Nesse caso, ter o auxílio de uma consultoria em cibersegurança pode fazer toda a diferença. Os especialistas serão capazes de indicar o nível de vulnerabilidade do empreendimento, assim como as melhores estratégias para superar as fraquezas cibernéticas do negócio.

### REGULAMENTO INTERNO DE SEGURANÇA

A empresa deve ter um regulamento interno de segurança da informação para agir de forma transparente com os seus usuários, garantir a confidencialidade de suas informações, atribuir responsabilidades, definir direitos, expectativas de acesso e uso das suas informações pelos usuários e terceirizados, definir mecanismos de controle e monitoramento da infraestrutura tecnológica para resguardar a segurança das suas informações e criar uma cultura educativa de proteção das suas informações.

### A INFRAESTRUTURA TECNOLÓGICA É DE EXCLUSIVA PROPRIEDADE DA EMPRESA

O uso de computadores e demais equipamentos da empresa devem ser apenas para fins profissionais, evitando o acesso a sites e o armazenamento de arquivos de cunho pessoal. Além disso, as contas corporativas fornecidas ao usuário devem ser intransferíveis.



## GOLPES COMUNS

Algumas estratégias de golpes são utilizadas repetidamente por criminosos, devido à eficácia dos métodos. Fique ligado nas principais táticas que estão sendo utilizadas ultimamente:

**PARENTE OU AMIGO PEDINDO DINHEIRO**
Utilizando a mesma foto de perfil de WhatsApp que um parente ou amigo da vítima, o criminoso entra em contato por mensagem, alegando ser a pessoa da foto e pedindo determinada quantia de dinheiro. Às vezes, até mesmo o número que aparece na conversa é o mesmo da pessoa que teve a identidade roubada.

**OPORTUNIDADE DE EMPREGO IMPERDÍVEL**
Por meio das redes sociais, WhatsApp ou SMS, os criminosos entram em contato com a vítima oferecendo uma vaga de emprego aparentemente irrecusável. É comum utilizarem o nome de multinacionais conhecidas, descreverem cargos de poucas horas de trabalho e oferecerem salários vantajosos.

**GOLPE DO ANIVERSÁRIO**
O criminoso entra em contato com a vítima fingindo ser uma loja e avisa que existe um presente ou brinde à espera do indivíduo. No entanto, para que a pessoa receba o mimo, ela deve pagar o "frete".

**FONTES:**
Ismael Júnior, consultor em cibersegurança
Cartilha de Boas Práticas em Segurança Cibernética da Federação das Indústrias do Estado de São Paulo (Fiesp)
Agência Gov

# PHISHING X RANSOMWARE:

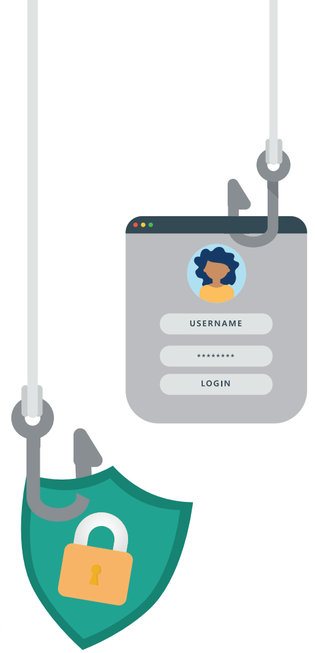
## DIFERENÇAS E SEMELHANÇAS ENTRE ESSES ATAQUES CIBERNÉTICOS


**INVESTIDAS HACKERS ATINGEM PESSOAS E ORGANIZAÇÕES NO MUNDO TODO. BRASIL ENCONTRA-SE NO CENTRO DOS ATAQUES, E POPULAÇÃO DEVE FICAR ALERTA**

Imagine-se num dia qualquer de trabalho, quando, de repente, ao utilizar o computador, uma mensagem surge na tela: seus arquivos foram criptografados e só serão liberados mediante o pagamento de um resgate. Esse é um caso clássico da atuação de ransomware, uma das principais táticas utilizadas por cibercriminosos, ao lado do phishing, para tirar vantagens de pessoas e organizações. Apenas os nomes, importados do inglês, já podem assustar muita gente. Mas os impactos para quem sofre esses crimes cibernéticos é ainda mais aterrorizante e podem ser devastadores para a saúde financeira e mental das vítimas.

Esses ataques cibernéticos compõem o rol de armadilhas da chamada engenharia social, definida pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) como a manipulação psicológica de indivíduos para obter informações confidenciais, acesso a sistemas ou dispositivos, ou para realizar ações que prejudiquem a si mesmos ou a terceiros.

Em resumo, trata-se de uma técnica de persuasão e manipulação, onde o engenheiro social explora falhas humanas, como confiança, ganância ou medo, para alcançar seus objetivos maliciosos. A seguir, entenda a diferença entre phishing e ransomware. (Lucas Casemiro)




OS ATAQUES COMPÕEM O ROL DE ARMADILHAS DA CHAMADA ENGENHARIA SOCIAL



### PHISHING: A ISCA ENGANOSA

**O termo phishing deriva da palavra inglesa *fishing* (pesca) e consiste em uma técnica de engenharia social que visa capturar informações confidenciais do usuário, como senhas, dados bancários ou números de cartão de crédito. Através de e-mails, mensagens de texto ou sites fraudulentos que imitam páginas legítimas, os criminosos induzem as vítimas a fornecer seus dados, muitas vezes explorando a urgência ou o medo.**

**Um dos principais diferenciais do phishing reside na sua natureza gradual. O ataque se desenrola em etapas, em que a vítima é "fisgada" por uma isca convincente e, gradativamente, cede suas informações sem perceber o real perigo.**

**Na prática, o phishing trabalha com gatilhos mentais com mensagens prometendo grandes ganhos, como "fique rico em um mês". Logo depois, vem outra mensagem: "você precisa fazer um depósito...". Existem muitas variações, e há casos em que alguns golpistas de fato pagam os primeiros ganhos, mas exigem investimentos cada vez mais altos das vítimas, que depositam valores proporcionalmente maiores, até que a comunicação é cortada e o golpe se efetiva.**

**"Sempre houve golpistas no mundo, mudou só a forma de agir. Enquanto no passado enganavam uma pessoa na rua, agora enganam milhares de pessoas através da Internet. Regra básica para não cair em phishing: ganhar dinheiro não é fácil, precisa de muito esforço. Hoje em dia o phishing é a maior maneira de iniciar um ataque cibernético. A maioria dos sistemas operacionais já possuem alguma proteção dos ataques conhecidos e a única maneira de entrar em uma empresa é através de um usuário", explica Marcial Fernández, professor em Ciência da Computação da Universidade Estadual do Ceará (Uece) e consultor em tecnologia do Governo do Ceará.**

## RANSOMWARE: O SEQUESTRO DIGITAL

Já o ransomware, por outro lado, é um software malicioso (malware) que se instala no dispositivo da vítima, criptografando seus arquivos e exigindo o pagamento de um resgate para liberá-los. O acesso a fotos, documentos importantes ou projetos profissionais é interceptado.

Mas ao contrário do phishing, o ransomware age de forma abrupta e direta. O ataque ocorre em um instante, deixando a vítima sem acesso aos seus dados e com a pressão do tempo para realizar o pagamento, geralmente em criptomoedas.

Um dos ataques mais devastadores da história do ransomware foi protagonizado pelo malware WannaCry. Infectando mais de 200 mil computadores em 150 países no ano de 2017, o ataque explorou uma vulnerabilidade da Microsoft não corrigida e causou danos estimados em 4 bilhões de dólares, atingindo empresas como Telefónica, Nissan, FedEx e Renault. O ataque gerou grande pânico e instabilidade, afetando hospitais, serviços públicos e infraestrutura crítica.

## IMPACTO

Os números mostram a efetividade dos ataques. Em 2023, cerca de 10% das organizações no mundo foram alvo de tentativas de ataques de ransomware. No Brasil, foram 75 empresas atacadas no período, sendo que 83% delas efetuaram o pagamento de resgate para reaver suas informações, de acordo com dados da empresa britânica Sophos, fornecedora de softwares e hardwares de segurança.

Ainda, segundo relatório do Fundo Monetário Internacional (FMI) divulgado em abril, os ataques cibernéticos a bancos, seguradoras e gestoras de ativos geraram perdas de US$ 12 bilhões ao setor financeiro global nas últimas décadas. Na economia global, o impacto do crime cibernético alcançou a casa dos U$ 8 trilhões em 2023, podendo aumentar para U$ 10,5 trilhões até 2025, calcula a empresa de investigação cibernética Cybersecurity Ventures.

Entre 2021 e 2023, o volume de ataques realizados no mundo só aumentou. Comparando 2023 com 2022, o aumento foi de 617%, com uma média de 544 ataques por minuto, segundo o Panorama de Ameaças da Kaspersky. No Brasil, o aumento no período foi de mais de cinco vezes.

## COMO PROCEDER EM CASOS DE ATAQUES?

**EM CASO DE PHISHING:**

**1. Mantenha a calma:** entrar em pânico não ajuda. Respire fundo e analise a situação com clareza.

**2. Não forneça informações:** jamais forneça senhas, dados bancários ou outras informações confidenciais em resposta a emails, mensagens, ligações telefônicas ou sites suspeitos.

**3. Verifique a autenticidade:** acesse o site oficial da empresa ou instituição supostamente remetente do email ou mensagem. Confirme se o link ou URL coincide com o site legítimo.

**4. Denuncie o ataque:** reporte o email ou site de phishing para as autoridades competentes, como o CERT.br (https://www.cert.br/), para que medidas sejam tomadas contra os criminosos.

**5. Altere suas senhas:** troque as senhas de suas contas de e-mail, banco e outras plataformas que podem ter sido comprometidas. Utilize senhas fortes e exclusivas para cada conta.

**6. Monitore suas contas:** acompanhe seus extratos bancários e históricos de compras para identificar transações fraudulentas.

**EM CASO DE RANSOMWARE:**

**1. Desconecte o dispositivo:** imediatamente, desconecte o computador, tablet ou smartphone da internet para evitar que o malware se espalhe para outros dispositivos da sua rede.

**2. Não pague o resgate:** pagar o resgate não garante a recuperação dos seus dados e pode incentivar a continuidade de ataques.

**3. Faça backup dos arquivos:** se possível, faça backup dos arquivos não criptografados em um dispositivo externo ou serviço de armazenamento em nuvem.

**4. Tente remover o malware:** utilize um antivírus atualizado para tentar remover o malware do seu dispositivo. Existem também ferramentas específicas para remoção de ransomware.

**5. Denuncie o ataque:** reporte o ataque às autoridades competentes, como o CERT.br (https://www.cert.br/), para que o caso seja investigado.

**6. Formate o dispositivo:** se a remoção do malware não for bem-sucedida, a última alternativa pode ser formatar o dispositivo, perdendo todos os dados não salvos em backup.

O Governo do Ceará também combate cibercrimes por meio da DRCC.
**Delegacia de Repressão aos Crimes Cibernéticos (DRCC)**
**Endereço:** Avenida Oswaldo Studart, 585, Fátima.
**Contatos:** (85) 3101-7586 / drcc@pc.ce.gov.br



## ESTRATÉGIAS PARA PROTEÇÃO DE DADOS PESSOAIS

**EMPRESAS**

> As empresas devem adotar diversas abordagens. Isso inclui aplicar soluções avançadas de segurança, como firewalls, sistemas de detecção de intrusões, controle de permissão nos sistemas, acesso baseado em autenticação multi-fator e criptografia de dados.
> Além disso, a capacitação dos funcionários é um aspecto fundamental, onde treinamentos regulares sobre práticas seguras de TI e conscientização sobre phishing são tópicos prioritários.
> Por fim, as empresas devem manter seus sistemas e software atualizados, realizando auditorias de segurança periódicas e definir planos de resposta a incidentes para mitigar os impactos de possíveis ataques.

**INDIVÍDUOS**

> Os usuários devem focar em três aspectos essenciais:
- Manter seus sistemas e aplicações atualizadas, possibilitando que vulnerabilidades identificadas sejam corrigidas;
- Habilitar a autenticação de dois fatores com senhas fortes, evitando que hackers possam usar informações prévias para ter acesso a conta do usuários, tais como data de nascimento, nome de parentes, etc; e
- Evitar clicar em links suspeitos e baixar anexos de e-mails sem conferir a procedência destes, prevenindo ataques de phishing.

**Fonte:** elaborado por Rafael Lopes, coordenador do Programa de Pós-graduação em Ciência da Computação da Uece.

## UMA SURPRESA DESAGRADÁVEL

Gilvando Silveira, funcionário público paraense radicado em Fortaleza, caiu em um golpe. Ao pesquisar sobre investimentos em criptomoedas, fez cadastros e foi informado que tinha sido contemplado com uma cota de participação. Um assessor de investimentos passou os dados da plataforma e, no Telegram, viu depoimentos que o incentivaram a investir R$ 10. Obteve retorno imediato de R$ 20. A plataforma então pediu mais investimentos em horários específicos, prometendo retorno dobrado ou triplicado ao fim do dia.

"Quando eu tinha investido mais de R$ 600 e tentei sacar, não conseguia. O assessor disse que eu só poderia sacar ao final do cronograma e se seguisse todos os horários", lamenta. "E o pior: compartilhei com familiares e o marido da minha sobrinha perdeu mais de R$ 9 mil", lamenta, relatando sensação de impotência.

# POR DENTRO
## DO FÁBRICA DE PROGRAMADORES

## CONHEÇA, ACOMPANHE E SE INSCREVA NESSA JORNADA PELO MUNDO DA LÓGICA ALGORÍTMICA

### CURSO DE EXTENSÃO APRENDENDO A PROGRAMAR COM GAMES

São apenas 2.000 jovens, especialmente estudantes de escolas de ensino médio do Ceará, que terão a oportunidade de aprender a construir um game, na versão 2024 do curso "Aprendendo a Programar com Games". O acompanhamento metodológico é feito pela Universidade Federal do Ceará. Cada grupo de 50 alunos terá um tutor. São videoaulas, aulões virtuais, fascículos digitais e radioaulas, com premiação para os melhores games desenvolvidos. Além disso, haverá uma emocionante festa de encerramento. As inscrições são gratuitas, foram abertas em 17 de junho e encerraram em apenas dois dias. Confira os outros produtos abertos ao público:

**4 LIVES**
Agosto e setembro
YouTube do O POVO

**4 PROGRAMAS DE TV**
Julho Na TV FDR

**6 WEBDOCS**
Agosto e setembro
YouTube do O POVO

**16 PODCASTS**
Agosto e setembro
Principais plataformas de streaming

**ACESSE O SITE**
**fdr.org.br/fabricadeprogramadores/**

## INSCREVA-SE NO WEBINAR CIBERSEGURANÇA

Dia 30 de julho, o Fábrica de Programadores realiza um webinar gratuito sobre cibersegurança. Apresentado pela jornalista Carol Kossling, o evento online está com inscrições abertas pela Sympla. Essa é uma oportunidade de aprofundar seu conhecimento em tecnologia e conhecer as melhores oportunidades da área.

**PAINEL 1**
**Tema: Cibersegurança Descomplicada**
**Palestrante:** Michel Bonfim, professor e pesquisador na UFC-Quixadá
**Minibio:** professor de Ciência da Computação na Universidade Federal de Ceará (UFC), Campus Quixadá. Possui Doutorado em Ciência da Computação no Centro de Informática (CIn) da Universidade Federal de Pernambuco (UFPE). Possui Bacharelado e Mestrado em Ciência da Computação pela Universidade Federal do Ceará (UFC), com estágio sanduíche na Universidade de Ottawa, Canadá. Tem experiência na área de Ciência da Computação, com ênfase em Redes de Computadores e Sistemas Distribuídos.

**PAINEL 2**
**Tema: O Mercado de Cibersegurança**
Palestrante: Pedro Prudêncio, professor de pós-graduação da UECE
**Minibio:** Pedro Prudêncio é um profissional com mais de 20 anos de experiência na área de cibersegurança. Atualmente, ocupa a posição de Diretor e Líder de Cyber Resilience em uma empresa multinacional. É professor em cursos de pós-graduação em diversas instituições renomadas, incluindo a Universidade Estadual do Ceará (UECE), a Universidade de Fortaleza (Unifor) e a Fundação Instituto de Administração (FIA).

**CONVIDADO 3:**
**Tema:** A Guerra Cibernética
**Palestrante:** Rafael Gonçalves Mota, professor e pesquisador na Unifor
**Minibio:** Prof. Dr. Rafael Gonçalves Mota é Advogado Criminalista. Pós-Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército Brasileiro. Pós-Doutorando em Estudos Marítimos pela Escola de Guerra Naval. Mestre e Doutor em Direito Constitucional pela Universidade de Fortaleza, onde é professor de direito penal e processo penal. Professor convidado da Escola Superior da Magistratura do Estado do Ceará, da Escola Superior de Defesa e da Escola Superior de Guerra. Possui curso de Inteligência Estratégica pela Escola Superior de Guerra da Colômbia e Escola Superior de Guerra do Exército do Peru. Palestrante nacional e internacional

**Debatedora:** Viviane Menezes, professora-adjunta UFC-Quixadá
**Minibio:** Possui doutorado em Ciência da Computação pelo Instituto de Matemática e Estatística da Universidade de São Paulo (2014) e graduação em Ciência da Computação pela Universidade Estadual do Ceará (2008) . Tem experiência na área de Ciência da Computação, com ênfase em Inteligência Artificial, atuando principalmente nos seguintes temas: planejamento automatizado, verificação de modelos e lógica temporal.

**INSCREVA-SE EM:**
https://www.sympla.com.br/evento-online/webinar-2-cibersegurança/2513598?referrer=fdr.org.br