



Como Combater Ladrões Digitais (Crackers)

Data: 03/05/2025

Elaboração: Carlos Andrade Ono – Fundador: Onocomp Marketing Digital & Publicidade

<https://www.onocomp.com.br/como-combater-ladros-digita-crackers/>

1. Proteja Suas Senhas

- **Nunca anote sua senha em locais visíveis ou arquivos, mesmo criptografados.**
- **Evite reutilizar senhas** em serviços diferentes, especialmente os de organizações distintas.
- **Não compartilhe sua senha**, mesmo com técnicos ou fornecedores - a menos que tenha certeza absoluta da identidade da pessoa.
- **Utilize senhas complexas**, com letras maiúsculas, minúsculas, números e símbolos, de no mínimo 8 a 11 caracteres ou mais.
- **Evite palavras de dicionário**, nomes próprios, datas de nascimento ou números de documentos.
- **Altere suas senhas periodicamente** e certifique-se de que novas senhas não sejam semelhantes às anteriores.

2. Use Gerenciadores de Senhas

Essas ferramentas ajudam a criar e armazenar senhas seguras. Opções populares incluem:

- **Bitwarden** – Gratuito, com recursos avançados.
- **LastPass** – Boa integração multiplataforma e recursos extras.
- **KeePass** – Código aberto, ideal para controle local.
- **Google Password Manager** – Integrado ao Chrome.
- **NordPass, RoboForm, iCloud Keychain** – Outras opções confiáveis.

Existem também os gerenciadores de senhas dos anti-vírus mas aí você fica preso a eles se for mudar de anti-vírus.

3. Ative a Autenticação de Dois Fatores (2FA) para tudo que tiver esta opção

Para quem hospeda sites com cPanel, a 2FA adiciona uma camada extra de segurança. No cPanel, vá em **Security > Two Factor Authentication**.

Hospedagens com DirectAdmin, AAPANEL, Plesk e demais sempre tem as medidas de segurança do carinho do TI.

Use o aplicativo **Google Authenticator**:

- [Android](#)
- [iPhone](#)
- [Google Chrome \(PC\)](#)

Não use a mesma senha para tudo.

Exemplo: Se a sua senha é a mesma para tudo você está vacilando e pedindo para ser assaltado(a).

<https://mail.google.com>

<https://facebook.com.br/>

<https://www.instagram.com/>

<https://www.tiktok.com>

Para cada conta de e-mail ou mídia social não é para gerar a mesma senha para todos.

Os ladrões se mesmo assim conseguirem roubar a senha do seu computador e ou do seu celular você se lascou pois ele pode fazer Spam e estragar todas as suas contas, além de monitorar a sua vida pessoal.

Use sempre autenticação de dois fatores e ou seja, depois da senha digitada você tem que confirmar algum código enviado por SMS ao seu número ou ao seu e-mail e ou usar algum app de dois fatores como o Google Authenticator por exemplo.

A cada dia os bandidos estão agindo e evoluindo nos roubos digitais e pedindo dinheiro / resgate para devolver arquivos confidenciais das empresas e das pessoas e ou até ameaçando entregar fotos e vídeos dos nudes das pessoas que fazem fotos e vídeos para enviar aos seus amantes; estas pessoas são alvos fáceis de bandidos digitais que sequestram os arquivos e conversas trocadas entre amantes e pedem dinheiro para não espalhar na internet e ou enviar para a esposa e ou marido.

Todo cuidado é pouco.

Ignore todo tipo de publicidade enganosa.

Não de margem para bandidos.

Não atenda com educação bandidos; quem mais cai nestes golpes são idosos e idosas de gerações diferentes da nossa geração atual que querem atender possíveis bandidos com educação. **Simplesmente DESLIGUE.**

Se for montar o seu site próprio com o seu programador, instale módulos e ou plugins de segurança com dupla autenticação; quais países podem acessar seu site e mude as portas de entrada ao seu site backend com um bom FIREWALL porque se o ladrão digital não sabe aonde está a porta ele não sabe aonde atacar e se o bandido é contratado pela sua concorrência para te atacar mas ele é de outro País ele bate com a porta na cara pois o site não irá abrir para ele.

Se mesmo assim você for atacado, restaure o seu backup de site.

Se você não faz backup do site e da segurança da sua empresa é vacilo seu.

4. Configure o BoxTrapper no cPanel

O **BoxTrapper** exige que remetentes desconhecidos confirmem seu envio antes de você receber o e-mail. Mantenha a **lista branca** (remetentes confiáveis) e a **lista negra** (remetentes bloqueados) atualizadas.

5. Use Antivírus Confiáveis

Evite antivírus gratuitos. Dê preferência para soluções pagas, como:

- **Norton** – Abrangente e confiável.

https://en-m-wikipedia-org.translate.goog/wiki/Norton_AntiVirus?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc

Sempre compre antivírus bom e pago não grátis. Os grátis não pegam tudo.

Norton é um bom antivírus use em todos os computadores, tablets, notebooks e celulares.

<https://br.norton.com>

- **Kaspersky** – Muito eficaz, mas envolto em polêmicas geopolíticas. – É feito na Rússia então como a Terra está com brigas entre países e partidos políticos pode dar ruim pra ti. Talvez você não queira a proteção de Comunistas que invadem suas máquinas e celulares.

https://en-m-wikipedia-org.translate.goog/wiki/Kaspersky_and_the_Russian_government?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt&_x_tr_pto=tc

Antivírus gratuitos é igual o barato sai caro os bandidos digitais dão risadas da sua cara.

Prefira os antivírus pagos e instalados em máquinas limpas e recém formatadas: Computadores, Notebooks, Tablets e também no seu Celular. Sim tudo tem que ter antivírus pago; proteger apenas uma porta da sua casa não é o suficiente tem que proteger a casa inteira; ou seja, todos os seus dispositivos.

6. Faça Backups Regulares

- Salve **banco de dados, arquivos, e-mails e documentos pessoais e empresariais** com frequência.
- Mantenha cópias locais e na nuvem.
- Atualize os módulos e plugins dos seus sites com frequência.

O carinha do TI ou seja, o técnico de informática e de segurança digital da sua empresa é quem faz isto; se você não tem um profissional destes, contrate quem é especialista nisto.

7. Cuidado com Golpes e Phishing

- **Nunca clique em links de fontes desconhecidas.**
- **Desconfie de mensagens alarmantes** via e-mail, WhatsApp ou SMS.
- **Não ligue para números 0800 recebidos de fontes duvidosas; Hoje em dia os bandidos tem uma central de operação em diversos países e até de dentro das cadeias se fazendo passar por funcionários de bancos e demais empresas só para te manipular e te botar medo e roubar seus dados, suas informações e o seu dinheiro.**
- Hackers podem operar até de dentro de presídios.
- Se for salvar senhas em navegadores; habilite sempre a mesma com dupla autenticação; caso você não faça isto por preguiça de ter que ficar digitando a senha a toda hora nos diversos sites, saiba que se um bandido entrar na sua máquina, ele rouba todas as suas senhas e faz da sua vida um inferno até apagando seus dados e ou monitorando a sua vida pessoal e empresarial. Evite instalar extensões em navegadores

pois extensões piratas roubam senhas. Evite entrar em sites perigosos, eles roubam suas senhas. Se desconfiar que o seu computador tem vírus faça backup de tudo e peça para formatar a máquina; isto costuma eliminar o risco de capturarem suas senhas.

Foi descoberto que plugins do navegador chrome possuíam trojans sem que ninguém soubesse.

Referência: <https://www.bleepingcomputer.com/news/security/malicious-chrome-extensions-can-spoof-password-managers-in-new-attack/>

- Crie uma política da segurança de entrada e saída dos seus funcionários; entrou crie as senhas para os mesmos e faça assinar uma política de segurança interna da empresa. Vai demitir o funcionário, troque todas as senhas dos e-mails, site e sistemas para com o mesmo(a) antes de avisar a demissão; Muitas empresas falham nisto e os ex-funcionários e ou ex-funcionárias por vingança apagam tudo e ou ficam monitorando os dados da sua empresa e vendendo para os concorrentes.

8. Bloqueie Ligações de Telemarketing

Cadastre-se no serviço **Não Me Perturbe** da Anatel. Use aplicativos para bloquear chamadas indesejadas:

- **Truecaller**
- **Whoscall**
- **Avast**
- **Hiya**
- **Should I Answer**
- **Calls Blacklist**
- **Call Blocker – Blacklist**

9. Conheça os Tipos de Hackers

- **Black Hat** – Criminosos cibernéticos.
- **White Hat** – Hackers éticos que ajudam a proteger sistemas.
- **Gray Hat** – Estão entre o bem e o mal.
- **Red Hat** – Combatem hackers Black Hat agressivamente.
- **Green Hat / Script Kiddies** – Iniciantes sem experiência técnica.
- **Hacktivistas** – Atuam com motivações políticas ou sociais.
- **Blue Hat** – Trabalham em empresas focando em segurança.

Os hackers são classificados em diferentes tipos, dependendo de seus objetivos e métodos. Os mais comuns são: White Hat, Black Hat e Gray Hat. Os White Hats, ou hackers éticos, usam seus conhecimentos para proteger sistemas, enquanto os Black Hats, ou hackers criminosos, o fazem para fins maliciosos. Os Gray Hats estão entre os dois, com suas ações podendo ser éticas ou não.

Tipos de Hackers:

- **White Hat (Chapéu Branco):**

Também conhecidos como hackers éticos, são profissionais de segurança que usam suas habilidades para encontrar vulnerabilidades em sistemas e ajudar a protegê-los. Eles trabalham para empresas e organizações, testando a segurança de sistemas e redes.

Black Hat (Chapéu Preto):

São hackers que usam seu conhecimento para fins ilegais e maliciosos, como invadir sistemas, roubar dados e causar danos.

Gray Hat (Chapéu Cinza):

Estão entre os White Hats e Black Hats. Podem violar políticas de segurança, mas geralmente não têm intenção de causar danos, podendo divulgar vulnerabilidades encontradas.

Red Hat (Chapéu Vermelho):

São hackers que buscam vulnerabilidades em sistemas e redes, mas com uma abordagem mais agressiva, podendo até mesmo usar táticas ofensivas para identificar problemas de segurança.

Blue Hat (Chapéu Azul):

São hackers contratados por empresas para testar a segurança de seus produtos e sistemas antes do lançamento, buscando vulnerabilidades e melhorando a segurança.

Script Kiddies:

Novatos em hacking que usam scripts e programas pré-existentes para realizar ataques, sem realmente entender como eles funcionam.

Cracker:

São hackers que se concentram em burlar sistemas de segurança e acessar informações, geralmente com motivações criminosas.

Hacktivistas:

Usam suas habilidades de hacking para divulgar informações, protestar contra governos ou empresas, ou apoiar causas políticas ou sociais.

Phreakers:

Especialistas em telefonia, que podem invadir sistemas de telefonia fixa e móvel para obter acesso a informações ou causar prejuízos.

10. Aumente Sua Proteção no Governo

- **Gov.br:** Bloqueie o uso indevido do seu CPF/CNPJ:
<https://www.gov.br/pt-br/servicos/impedir-permitir-participacao-do-meu-cpf-no-cadastro-nacional-de-pessoas-juridicas-cnpj>
- **INSS:** Bloqueie a contratação de empréstimos consignados em seu nome.
Para bloquear a contratação de empréstimos consignados em seu nome, você pode usar o aplicativo ou site Meu INSS, ou ligar para a Central 135 do INSS. Ao bloquear o benefício, você impede que novos empréstimos consignados sejam contratados em seu nome, protegendo-se de fraudes e contratações não autorizadas.
<https://meu.inss.gov.br/#/login>

Sempre faça backup dos seus sites e arquivos da empresa e ou seja:

- Banco de Dados + Arquivos
- Atualize sempre os módulos do seu site
- Faça backup dos arquivos e aplicações de sua empresa

- Sempre invista em segurança pois nunca se sabe quando você será roubado e o ladrão pode estar em qualquer ponto do planeta terra te atacando para roubar dados, usar a sua infraestrutura para praticar golpes em outras pessoas e você sendo o laranja.

Investir no departamento de tecnologia da informação e segurança é crucial; quem ignora isto vira alvo de bandidos e eles dão risadas te chamando de vacilão e ou vacilona.

11. Use gravadores de voz e de chamadas telefônicas tanto no fixo como em seu celular

Quando você investe em URA's e Apps de gravações de chamadas telefônicas você gera provas para se proteger contra bandidos te ligando e se passando por funcionários e até contra estelionatários que não cumprem o que foi combinado por chamada telefônica; Muitas das empresas que falam que estão gravando a ligação não te enviam o arquivo da mesma se a ligação for contra a atuação da mesma; elas dão uma de pilantras.

Ex-funcionários de bancos e operadoras telefônicas e demais segmentos aonde os funcionários tinham acessos aos nossos dados pessoais em geral podem cometer crimes com estes dados se unindo a bandidos digitais.

Com o advento da Inteligência Artificial que clona a sua VOZ, IMAGEM e demais cenários; evite ficar atendendo ligações de estanhos e já sair falando pois sua voz pode estar sendo clonada.

12. Evite postar tudo na internet e seus paradeiros e viagens

Os bandidos digitais adoram roubar ciclistas e corredores que postam o mapa e as fotos de onde fazem sempre o seu percurso; além das viagens exuberantes.

A pesca dos bandidos agora é outra, saber da sua vida para te assaltar no digital.

13. Golpe do Amor

O "golpe do amor" é uma forma de estelionato onde o criminoso finge ter um relacionamento amoroso com a vítima para obter dinheiro ou outros benefícios. Os golpistas usam perfis falsos, tanto em plataformas de relacionamento Exemplo: TINDER; como nas redes sociais, para enganar e conquistar a confiança da vítima.

Referência:

<https://www.cnnbrasil.com.br/nacional/golpista-do-tinder-e-presos-suspeito-de-fazer-37-vitimas-no-df/>

Filme:

O Golpista do Tinder

<https://www.netflix.com/br/title/81254340>

Como funciona:

Criação de perfis falsos:

Os golpistas criam perfis com fotos e informações falsas para se passarem por alguém que atrai a vítima.

Conquista da confiança:

Eles se aproximam da vítima, demonstram interesse e desenvolvem um relacionamento, geralmente a distância, para ganhar a confiança.

Pedido de dinheiro:

Após conquistar a confiança, os golpistas pedem dinheiro para diversos fins, como ajuda em dificuldades financeiras, investimento em negócios ou viagem.

Exploração financeira:

A vítima, acreditando na relação, cede ao pedido e transfere dinheiro, que geralmente é usado pelos criminosos.

Sinais de alerta:

Perfil com poucas informações:

Perfil com poucas fotos, sem informações detalhadas ou inconsistências.

Desejo de relacionamento rápido:

O golpista busca avançar rapidamente na relação e evita encontros presenciais ou videochamadas.

Pedidos de dinheiro frequentes:

Pedidos de dinheiro para diversos fins, sem comprovação das dificuldades.

Ausência de amigos em comum:

O golpista pode não ter amigos em comum com a vítima ou não conseguir confirmar a identidade.

Como se proteger:

Verifique a identidade do perfil:

Pesquise fotos e informações do perfil na internet para identificar se são falsas ou se a pessoa é real.

Procure informações sobre a pessoa:

Converse com amigos ou familiares que possam conhecer a pessoa para confirmar a autenticidade do perfil.

Não compartilhe informações pessoais:

Evite compartilhar informações financeiras, senhas, endereço ou dados bancários com pessoas que você não conhece pessoalmente.

Seja cauteloso com pedidos de dinheiro:

Desconfie de pedidos de dinheiro, especialmente se a pessoa for desconhecida e não apresentar provas das dificuldades.

Denuncie:

Caso suspeite de um golpe, denuncie o perfil ou a pessoa às autoridades competentes.

14. Dica de Filmes:

Piratas da Informática

<https://www.adorocinema.com/filmes/filme-133537/>

Criptofraude

<https://www.adorocinema.com/filmes/filme-324345/>

Roubo Cibernético: Bilhões em Bitcoins 2024 Trailer Oficial Dublado

<https://www.youtube.com/watch?v=F3cURdTc22c>

Crypto

<https://www.primevideo.com/-/pt/detail/Crypto/0N0ZH8YV48OT7Y00JS9F7XSJ6W>

Como Ficar Rico

Mostra a máfia das pirâmides financeiras e as pessoas enganando as outras via internet e o mentor mostrando em como se livrar destas pirâmides de marketing multinível

<https://www.netflix.com/br/title/81410436>

Hackers no Controle

<https://www.adorocinema.com/filmes/filme-309023/>

Sociedade Hacker

<https://www.primevideo.com/-/pt/detail/Sociedade-Hacker/0SJJSQE04USSW0CM5BMESSR1IG>

STARTUP

<https://www.primevideo.com/-/pt/detail/StartUp/0IZG0WDVB00U4HRHOEXSO2MDMXA>

Principais Filmes Sobre Hackers no Mundo Digital

Clássicos e Cult

1. **WarGames (1983)**

- Um jovem hacker invade, sem querer, um sistema militar e quase inicia a Terceira Guerra Mundial.

2. **Hackers (1995)**

- Um grupo de adolescentes hackers descobre uma conspiração corporativa. Filme icônico da cultura hacker dos anos 90.

3. **Sneakers (1992)**

- Especialistas em segurança são forçados a roubar um dispositivo de decodificação muito poderoso.

4. **The Net (1995)**

- Uma analista de sistemas tem sua identidade apagada após descobrir uma conspiração digital.

Tecnologia e Cibercrime

5. **Swordfish (2001)**

- Um hacker é recrutado por um agente misterioso para roubar bilhões do governo.

6. **Live Free or Die Hard (2007)** (*Duro de Matar 4.0*)

- Um ataque hacker em larga escala ameaça destruir a infraestrutura dos EUA.

7. **Blackhat (2015)**

- Um hacker condenado é liberado para ajudar o governo dos EUA a encontrar cibercriminosos globais.

Baseado em Histórias Reais

8. **Pirates of Silicon Valley (1999)**

- Mostra o surgimento da Apple e da Microsoft, com foco em Steve Jobs e Bill Gates, e a “cultura hacker” dos primórdios da computação.

9. **The Fifth Estate (2013)**

- Conta a história da fundação do WikiLeaks por Julian Assange.

10. **Citizenfour (2014)** (*documentário*)

- A história real de Edward Snowden e a revelação de programas de vigilância global da NSA.

Ficção com Temas Hacker

11. **The Matrix (1999)**

- Embora mais voltado para ficção científica, o personagem principal é um hacker que descobre a natureza simulada da realidade.

12. **Tron (1982 / 2010)**

- Um programador é sugado para dentro do mundo digital que ele ajudou a criar.

Hacktivismo e Anonimato

13. **Who Am I: Kein System ist sicher (2014)** (*alemão*)

- Um jovem hacker busca fama, mas se envolve com crimes cibernéticos e espionagem internacional.

14. **We Are Legion: The Story of the Hacktivists (2012)** (documentário)

- Explora os movimentos Anonymous e o hacktivismo moderno.

15. **E-mails / SMS / WhatsApp Mensagens / Messenger e demais comunicadores de Pescaria:**

Os ladrões digitais vivem mandando e-mails falsos com notificações falsas para os PEIXES = BOBO(AS) Caírem e muitas caem nos golpes; e-mails com Boletos Falsos para pagar de diversas empresas e instituições, e-mails com notificações judiciais para cumprir, e-mails de bancos com notificações dos gatilhos mentais diversos que fazem as pessoas ficarem preocupadas. Os ladrões estão se lixando para os PEIXES; eles querem é roubar os seus dados, a sua grana e principalmente o seu tempo de vida.

Pessoas sensíveis a estas mensagens pensam que são verdadeiras a mensagem e caem na pescaria dos bandidos clicando em links com IPS FALSOS, ligando para o 0800 dos bandidos e os mesmos dando risadas destes PEIXES.

Simplesmente ative o seu ANTI-SPAM de e-mail e demais proteções, apaguem mensagens falsas e NÃO leia por completo, investigadores experientes já sabem identificar o código da mensagem e sabe que é PESCARIA para PEIXES.

Aprenda a deletar e bloquear as mensagens de WhatsApp e se desconhece, simplesmente DENUNCIE SPAM e BLOQUEIA A PESSOA, Ladrões estão loucos para iniciar conversas com PEIXES BOBO(AS) e ludibriarem as mesmas.

Não caia no conta do vigário.

Não caia no conto da sereia.

Não caia nas solicitações de ONG ´s Falsas; no Brasil o que mais se criou foram ONG ´s com o objetivo de ajudar pessoas carentes e demais outros objetivos mas não se criou um departamento para auditar todas estas ONG ´s que muitas das vezes estão agindo de má Fé e roubando o seu rico dinheirinho.

Não caia em ligações de pessoas se fazendo passar por terceirizada do SEBRAE e já sair perguntando qual é o seu faturamento e afins; os ladrões dão TROTES DIVERSOS POR Diversos meios de comunicação e são dissimulados e mau caráter, o objetivo é único te ROUBAR e Lesar com a sua vida e o seu tempo de trabalho; quem cai nestas arapucas / armadilhas são os vacilões da vez.

Se você entrou no funil de marketing de alguma empresa e ou produtor(a) digital irá entrar no grupo de whatsapp dos mesmos; saiba que irá ser bombardeado de mensagens com os diversos tipos de gatilhos mentais tanto no whatsapp como por e-mail então se não gostar simplesmente se descadastre para parar de receber as várias mensagens por email e pronto; se assim não for feito, reclama no registro.br / procon / reclameaqui e no google meu negócio da pessoa. Quanto aos grupos de whatsapp, simplesmente bloqueia o contato e sai do grupo; muito infoprodutor é sem noção e fica te enchendo o saco até no seu número privado; Bloquear é uma saída; se insistirem a encher o saco vindo de outros números bloqueia também e denuncie, se puder printa todas as conversas e manda para o WhatsApp Suporte reclamando de importunação pessoal.

Só entre em grupos se você pedir para participar, acordar no outro dia com o seu número de WhatsApp estando em grupos que você não solicitou e chato. Bloqueia nas configurações do WhatsApp para não deixar ninguém te incluir em grupo nenhum sem a sua permissão. Eles e Elas Atacam e você tem que se proteger sempre.

Oriente que quem for te incluir em grupo, adicione o seu número na agenda e manda um Oi para assim você colocar o contato na sua agenda e assim ela poder te incluir no grupo e ou mandar o link para entrar no grupo; não é assim bagunçado chegar chegando na força bruta do pilantra.

Bloqueia no WhatsApp todas as mensagens não solicitadas de contatos que não estão na sua agenda os pilantras adoram fazer um SPAM e pescar PEIXES BOBOS.

Hoje em dia não dá para ficar sendo manso com bandidos digitais, tem que sabe ser proteger e se possível ter um profissional de segurança digital contratado para combater estes bandidos.

16. **Empresas que intermediam as vendas**

Empresas como Hotmart, Kiwify, Eduzz e demais no mercado, cobrem delas no painel das mesmas um histórico de tudo o que você comprou de cursos e afins; algumas delas não tem em seu painel um histórico das compras por você efetuadas e assim os bandidos digitais verificam estas falhas e usam as mesmas para venderem e sumirem do mapa com as suas áreas de membros externas.

Conclusão

A segurança digital deve ser uma prioridade para todos. O uso de senhas fortes, autenticação de dois fatores, backups regulares e antivírus confiáveis pode prevenir prejuízos financeiros, vazamentos de dados e outros danos sérios que quebram a sua vida e fecham muitas empresas; aprenda a investigar e se defender auditando a tudo e todos.

Investir em tecnologia da informação é investir em tranquilidade. Não espere ser vítima para agir.

Elaboração: Carlos Andrade Ono – Fundador: Onocomp Marketing Digital & Publicidade

<https://www.onocomp.com.br/como-combater-ladros-digitais-crackers/>