PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina
Gabinete da Presidência
Núcleo de Inteligência e Segurança Institucional

CARTILHA DE SEGURANÇA CIBERNÉTICA

Prevenção e orientações contra crimes cibernéticos

Apresentação

Os avanços tecnológicos trazem novos desafios ao profissional do direito no que diz respeito às providências a serem tomadas quanto à busca de dados na internet. Nesse cenário de multiplicação de crimes informáticos próprios e impróprios, há a necessidade da correta atuação do profissional de direito na preservação da evidência eletrônica, na atribuição de autoria e na remoção de conteúdo (BARRETO, 2019).

Contudo, a grande quantidade de informações recebidas a cada dia impossibilita o conhecimento de todos os serviços e plataformas disponíveis, das novas modalidades de crimes, da legislação aplicável e das providências para denunciar ou remover um conteúdo ilegal ou abusivo (BARRETO, 2019).

Por outro lado, a compreensão do tema se impõe aos demais profissionais do direito, em especial aos aplicadores da lei e julgadores, como forma de qualificar mais ainda a abrangência do ato legal e de assegurar o emprego de medidas de autoproteção de maneira eficiente e eficaz.

O **Núcleo de Inteligência e Segurança Institucional do Tribunal de Justiça de Santa Catarina (NIS)**, criado pela **Resolução GP n. 10 de 21 de março de 2018**, tem como atribuições:

> entre outras, planejar e executar atividade profissional de proteção de magistrados, de seus familiares e de servidores em situação de risco decorrente do exercício da atividade funcional; adotar e recomendar medidas de prevenção para a redução das vulnerabilidades; fomentar a cultura da segurança institucional entre os membros do Poder Judiciário do Estado de Santa Catarina; e desenvolver rotinas de boas práticas em segurança institucional (TRIBUNAL DE JUSTIÇA DE SANTA CATARINA, 2018).

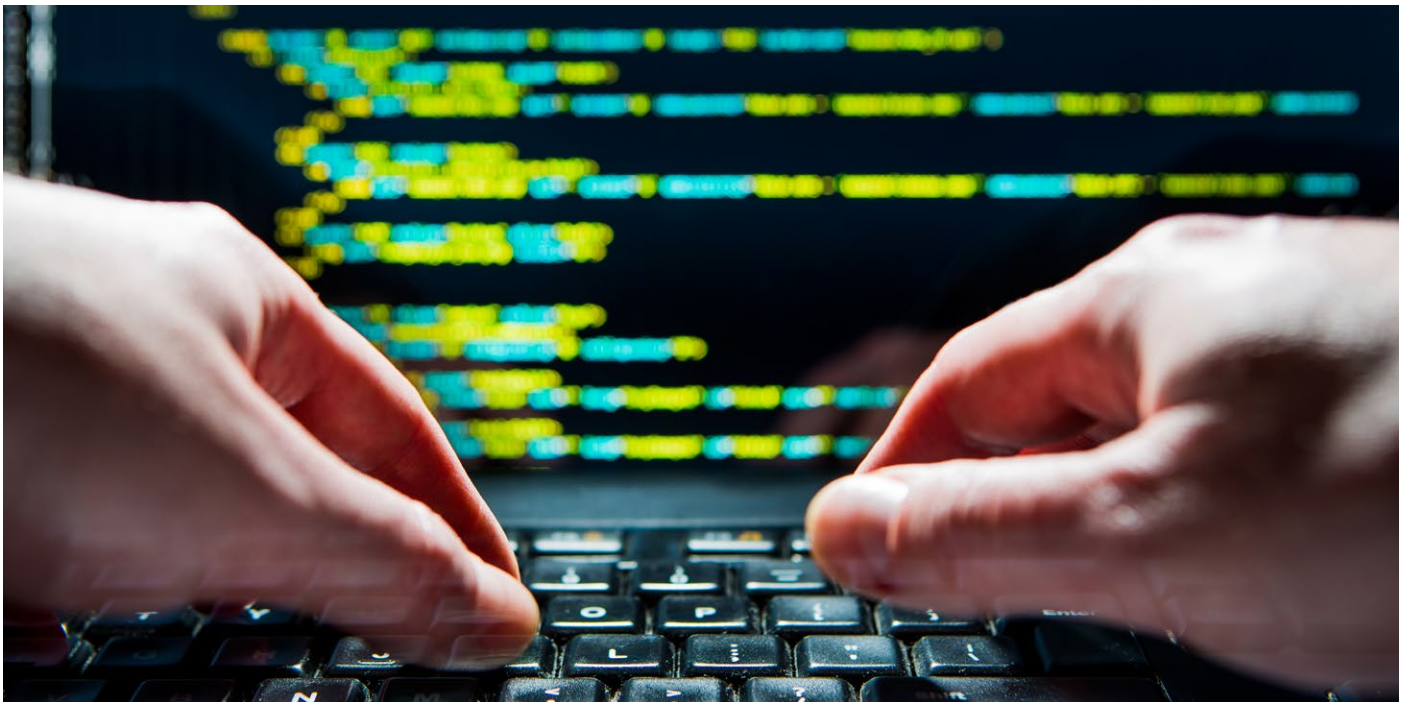
A proteção a magistrados, familiares e servidores do Poder Judiciário catarinense também se dá no mundo virtual, sendo imprescindível a adoção de medidas de segurança nos dispositivos eletrônicos, sites e redes sociais, visando mitigar o acesso indevido a dados sensíveis e sigilosos, sejam pessoais ou institucionais.

A segurança digital depende de cada usuário, sendo necessário cuidado permanente.

> “A segurança é apenas uma ilusão, uma falsa sensação, que fica cada vez maior quando entram a inocência e a ignorância humana. A segurança não é um produto, e sim um processo, ou seja, é um problema além da tecnologia.” (MITNICK, 2016)

A **Divisão de Inteligência do NIS** pretende com este material alertar e auxiliar o público-alvo com indicação de medidas que, se observadas, poderão diminuir consideravelmente as chances de alguém ser vítima em um golpe ou ataque virtual.

É importante destacar que, conceitualmente, a segurança da informação está diretamente relacionada à proteção de um conjunto de informações no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São propriedades básicas da segurança da informação a confidencialidade, a integridade, a disponibilidade, a autenticidade e a legalidade.



Segurança em dispositivos eletrônicos: smartphones (Android e IOS), notebooks e computadores em geral, tablets, smartwatches e dispositivos “vestíveis” em geral (IoT).

MEDIDAS DE SEGURANÇA

Enquanto está na posse do celular[1]

1. Tenha guardado marca, modelo, IMEI e número de série do seu aparelho (geralmente essas informações estão disponíveis na caixa do aparelho). Anote também o PIN e PUK do chip (vem no cartão entregue pela operadora).

2. Utilize um bom código alfanumérico (letras e números). Evite padrões de desenho "screenlocks" (em Android) ou códigos numéricos como "1234", "0000" ou afins. Jamais use um telefone sem código de bloqueio.

3. Utilize autenticação de dois fatores em todas as suas contas de redes sociais e serviços de Internet (Facebook, Instagram, Twitter, Gmail, Icloud etc).

4. Habilite a autenticação de dois fatores via PIN (código) no aplicativo do WhatsApp (Ajustes › Conta › Confirmação em duas etapas). Evitando assim golpes frequentes como simcard swap.

5. Sempre habilite o Touch ID (leitor de impressões digitais), reconhecimento facial ou senha para todos os aplicativos que suportam.

6. Habilite o PIN (código) do chip (no iPhone esta configuração fica em Ajustes › Celular › PIN do SIM). Dessa forma, será solicitada uma senha sempre que seu chip for colocado em outro aparelho. Lembrando que o chip já vem com um PIN (código) da operadora, que será necessário para alterar. Os padrões são: Vivo 8486; TIM 1010; Claro 3636; Oi 8888, sendo que o mais indicado é verificar no cartão do qual o chip é destacado quando recebido. **Todo cuidado é pouco aqui, pois é muito fácil bloquear o chip ao tentar desbloqueá-lo incorretamente 3 vezes. Neste caso, só ligando para a operadora, ou usando o PUK (segundo código de segurança fornecido pela operadora) para desbloquear.**

7 Desabilite a visualização do conteúdo de notificações em geral quando o aparelho estiver bloqueado. Essa medida é muito importante e evita que o criminoso tenha acesso aos códigos, mensagens e e-mails recebidos recentes.

8 Desabilite a Siri (iOS) na tela bloqueada (Ajustes › Siri › Permitir Quando Bloqueado). Do contrário, basta que alguém pergunte "Qual o meu nome?" para saber seu nome, telefone, empresa (dependendo do que constar no seu contato).

1 Fonte: Mercês (2019).

Depois de furto/roubo ou perda do celular[2]

1 Ligue para a sua operadora e informe o ocorrido. A operadora irá bloquear o chip.

2 Cancele seus cartões de crédito que estejam vinculados ao aparelho (Apple Pay, Android Pay, Samsung Pay, dentre outros, há casos em que ladrões utilizaram Apple Pay e similares para fazer compras ou mesmo pediram comida em aplicativos como iFood e Uber Eats).

3 Faça um boletim de ocorrência na delegacia mais próxima ou pela Internet. Você vai precisar dos dados de seu aparelho: marca, modelo, IMEI e número de série.

4 Desconecte o dispositivo das suas contas de e-mail, redes sociais e outros serviços (é impossível enumerar todos, mas serviços comuns são Gmail, Facebook, Instagram, Twitter, Spotify, etc).

5 Programe para deletar os dados pelo site do fabricante (Google, Apple, etc).

2 Fonte: Mercês (2019).

Dicas para criação de senha nos diferentes sistemas operacionais e tipos de dispositivos

1		Sistema operacional IOS ➤ Senhas fortes, Configuração de bloqueio de conteúdo das notificações, Segurança de tuas etapas na conta Icloud, localização de dispositivo habilitada.
2		Sistema operacional Android ➤ Senhas fortes, evitar desenhos (screenlock), criptografia no micro SD (cartão de memória), caso utilize.
3		Notebooks e Computadores: Senhas fortes, antivírus, webcam sempre coberta, criptografia do HD quando possível.
4		Smartwatchs (relógios inteligentes) ➤ Configuração de senha ou padrão de bloqueio de tela para evitar acesso indevido.
5		Internet das Coisas (IOT): Segurança de dispositivos inteligentes em casa, como Câmeras IP de Segurança, veículos, fechaduras digitais, geladeiras, televisores, etc.

Crie uma senha forte

O uso de senhas fortes é medida de segurança básica, pois é sabido que o usuário tende a utilizar senhas fáceis para rápido desbloqueio do aparelho. **Na sequência pode-se verificar dados apresentados por Silva (2019) e pela National Cyber Security Centre (2019) acerca da utilização de senhas.**

A senha mais comum no mundo é “123456”, usada para acessar 23,2 milhões de contas e serviços online ao redor do mundo. E a segunda senha mais escolhida pelos usuários globalmente é uma variação um pouco maior da mesma ideia, com 7,7 milhões de contas podendo ser acessadas pela senha “123456789”.

A maior parte das senhas utilizadas que compõem o top 20 utiliza uma mistura de números e letras que seguem a mesma lógica das cinco mais utilizadas, como “abc123”, “000000” ou “password1”.

Evite informações pessoais, como data de nascimento, número de telefone, número do RG ou CPF, pois com o uso de engenharia social, sua senha pode ser descoberta utilizando outro tipo de ataque conhecido como força bruta, que consiste em uma lista de palavras/números e diversas tentativas até encontrar a combinação que desbloqueie seu aparelho.

CLONAGEM DE CONTA DO WHATSAPP

Golpes com clonagem de SimCard

Criminoso solicita recuperação de SimCard da vítima.

Instala o aplicativo WhatsApp e recebe código de autenticação.

Assume a identidade da vítima.

Alega emergência e solicita empréstimos aos contatos em grupos ou individualmente.

Informa conta de terceiros para depósito.

Modus operandi

Utilização de funcionários ou terceiros com acesso ao banco de dados das operadoras para o resgate do chip.

Uso de documento falso por criminosos em lojas físicas. Obs.: Como regra, a recuperação de SimCard em todas as companhias exige a presença do cliente na loja física.

Procedimentos de recuperação de conta

Registrar boletim de ocorrência

Avisar aos seus contatos e familiares sobre a fraude

Bloquear por telefone o SimCard na operadora

Encaminhar e-mail para support@whatsapp.com (em português) e solicitar o imediato bloqueio da conta de usuário

Iniciar a conta no whatsapp com o novo código de verificação.

Criminoso habilitou verificação em 2ª etapa

Após recuperar o chip e registrar novamente a conta no WhatsApp, digite erroneamente códigos sucessivos a fim de suspender a conta por um prazo de 7 dias.

Passado esse período, o usuário deverá registrar a conta novamente e receberá um novo código de ativação via SMS.

Após esses passos, o uso será normalizado.

Clonagem da conta de Whatsapp através de engenharia social em sites de compras

O usuário anuncia um produto em site de comércio eletrônico e divulga o número de telefone para contato.

O golpista envia uma mensagem para o WhatsApp do anunciante, comunica ser da empresa de comércio eletrônico e solicita a atualização de dados cadastrais.

O golpista solicita o fornecimento do código de seis dígitos, repassado por SMS.

Após o envio do código pelo usuário, o criminoso consegue acessar a conta do WhatsApp dele e solicitar empréstimos em dinheiro aos seus contatos.

Nesse caso, não há a recuperação indevida do SimCard; o golpe se restringe apenas à clonagem do número no aplicativo.

Orientações para as vítimas

1. Registre ocorrência policial.
2. Avise aos seus contatos e familiares da fraude.
3. Envie e-mail para support@whatsapp.com. No assunto, escrever: Perdido/Roubado: "Por favor, desative minha conta". No corpo da mensagem, colocar o número de telefone com o código do país: Ex.: +55 48 99999-9999. A empresa WhatsApp irá desativar a conta da vítima, que só poderá ser utilizada após 7 dias.
4. Quando o golpista tiver habilitado a verificação em duas etapas, reinstale o número no aplicativo e digite erroneamente códigos sucessivos até bloquear a conta. Após determinado período, o titular receberá um novo SMS.

DICAS

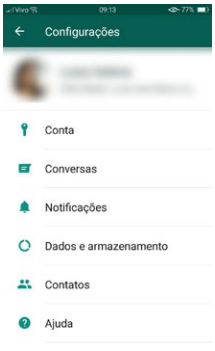
- Habilite a verificação de segunda etapa no aplicativo WhatsApp.
- Não repasse nenhum código fornecido por SMS, nem qualquer outra informação sem confirmação com o setor responsável das empresas através dos canais de atendimento.
- Fique atento aos dados conflitantes na mensagem recebida.
- Como regra, as grandes empresas de compra e venda na internet não mantêm contato com os clientes através de aplicativos de mensagem.

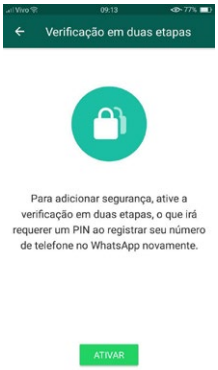
Proteja sua conta, habilite verificação de 2ª etapa

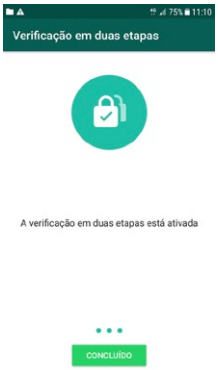
Os golpes praticados com a clonagem de SimCard aumentaram consideravelmente nos últimos meses. A habilitação por parte do usuário de verificação de 2ª etapa da conta do WhatsApp dificulta a atuação do criminoso.

Android

Configurações › Conta › Verificação em duas etapas › Ativar › Inserir código PIN com seis dígitos › Informe e-mail para recuperação.

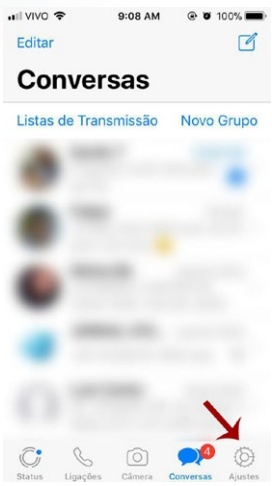


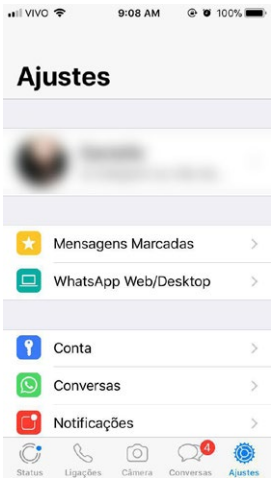


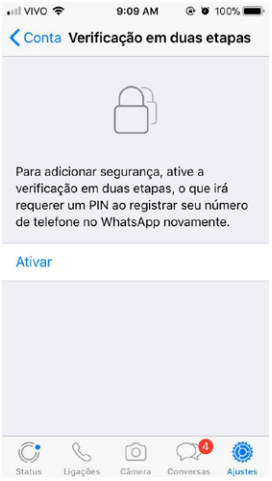


IOS

Acesse o WhatsApp ❯ Ajustes ❯ Conta ❯ Verificação em duas etapas Ativar ❯ Inserir código PIN com seis dígitos ❯ Informe e-mail para recuperação.







QRL Jacking

Espelhamento Indevido do WhatsApp

Nessa modalidade, os criminosos criam páginas de *phishing* com QR Code do WhatsApp e, através de engenharia social e estando na mesma rede da vítima, conseguem capturar a sessão do aplicativo quando esta faz o login através do WhatsApp Web ou Desktop.

A vítima utilizará o aplicativo no seu smartphone, todavia o criminoso acessará o WhatsApp Web e conseguirá ver o conteúdo das conversas dela.

1  Não escaneie QR Code em sites desconhecidos.

2  Acesse o app apenas pelo WhatsApp Web ou na versão desktop.

3  Evite utilizar o WhatsApp Web em conexões públicas ou pouco confiáveis.

4  Verifique com frequência as sessões ativas no seu smartphone.

5  Mantenha a versão do WhatsApp atualizada.

PRESERVAÇÃO DA EVIDÊNCIA CIBERNÉTICA COM ATA NOTARIAL

Conceito

É instrumento dotado de fé pública lavrado por tabelião a pedido de terceiro interessado. Poderá ser utilizado no ambiente cibernético para garantia da preservação e integridade das evidências nele produzidas.

PREVISÃO LEGAL Art. 384 do CPC – A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião. Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.

Preservação da evidência

Procedimento

1. Deve ser lavrada por tabelião a pedido de terceiro
2. Indicar os procedimentos utilizados na obtenção do dado
3. Descrever o fato com relato detalhado do que se vê e ouve
4. Salvar o conteúdo em mídia a fim de acompanhar o documento lavrado

5 Maneiras de garantir a guarda de dados pelas aplicações de internet

1. Print Screen

A captura de tela é uma das opções mais utilizadas para salvar um conteúdo da tela de um dispositivo informático. No entanto, apesar de guardar alguns elementos essenciais, peca por omitir outros relevantes para atribuição de autoria. Recomenda-se sua utilização em último caso.

2. Certidão Policial

- Lavrada pelo escrivão de polícia a requerimento da parte interessada
- Passo a passo na obtenção dos dados
- Descrição do fato
- Dados da aplicação de internet (perfil, página, usuário, ID ou URL) onde se encontra o conteúdo
- Salvaguarda da imagem, vídeo e áudio em meio digital
- Não se confunde com a perícia.

3. Ata Notarial

- Previsão Legal: art. 384 do CPC
- Dotada de fé pública
- Lavrada por um tabelião
- Não pode emitir opinião, juízo de valor ou conclusão
- Recomendamos os mesmos procedimentos para lavratura da certidão.

4. Ofício Autoridade Policial

- Previsão legal: art. 15, § 2º, do Marco Civil da Internet; art. 6º, I e III, do CPP.
- Requisita a preservação dos registros de acesso.
- Identifica no documento a URL, perfil, página, conta de e-mail ou outro dado relacionado.

5. Facebook Records

- Acessível em www.facebook.com/records
- Preserva os dados do Facebook e do Instagram.
- Quem pode solicitar a guarda dos dados: Polícia, Ministério Público e Poder Judiciário.
- Advogado não pode pleitear por esse canal.
- As solicitações devem ser realizadas por e-mail institucional.

CONTA DO INSTAGRAM HACKEADA

Perda de Acesso ao Instagram e Procedimento para Recuperação de Perfil

Caso tenha perdido acesso ao Instagram, vá até a conta de e-mail vinculada ao aplicativo e localize a mensagem informando sobre a modificação. Desfaça essa alteração.

Para a Perda de Acesso no Instagram e no E-mail Vinculado existem duas possibilidades:

1. Havendo indícios de crime e após o registro de ocorrência, a autoridade policial poderá requisitar, através de ofício, a recuperação da conta (deve apontar e-mail para novo acesso);

2. Denunciar uma conta. Denunciar Conta Invadida no Instagram. No Android, na tela de login, clicar em obter ajuda para entrar". No IOS, na tela de login, clicar em "Esqueceu a senha?".

Obs.: O Instagram enviará um e-mail para verificação de identidade

Dicas de segurança

- Sua senha é pessoal e intransferível.
- Use senhas distintas para acessar e-mail e Instagram.
- Remova as permissões de aplicativos de terceiros.
- Habilite a verificação em duas etapas.

Fonte: https://help.instagram.com/

Recuperar conta hackeada no Instagram

Não tenho mais acesso à conta

Caso não consiga mais acessar a sua conta no Instagram, recomenda-se verificar o e-mail vinculado ao perfil e tentar desfazer a alteração. Não logrando êxito, denuncie o fato diretamente no aplicativo.

Recuperar conta Android

Na tela inicial do aplicativo, clique em "obter ajuda". Insira o nome de usuário, e-mail ou telefone e depois clique em Avançar. Um e-mail será enviado com outras etapas da recuperação.

Recuperar conta IOS

Na tela inicial, clique em "Esqueceu a senha?". Depois acesse "Precisa de mais ajuda?". Um e-mail será enviado com outras etapas da recuperação.

Ofício da autoridade policial

Nos casos de instauração de inquérito policial, o delegado de polícia poderá enviar ofício diretamente ao Instagram solicitando a recuperação de conta através da plataforma Facebook Records.

Dicas de segurança

- Ative verificação de duas etapas.
- Não compartilhe senhas.
- Troque suas senhas com frequência.
- Evite a autorização de aplicativos de terceiros.

PERDA DE ACESSO EM REDE SOCIAL E E-MAIL

Registro de Boletim de Ocorrência

Quando ocorre a prática de crimes em conta de e-mail ou rede social hackeada, algumas informações devem estar presentes para auxiliar na individualização da autoria delitiva:

1. Data, hora e local do último acesso, com redes wifi ou conexões de internet utilizadas.
2. Conta de e-mail vinculada.
3. Relatos da conta utilizada para postagens ou envio de e-mail. Indicar os dispositivos informáticos utilizados para acessar a conta (celular, PC, notebook, etc.) e se houve a utilização de equipamento de terceiros para tal.
4. Em perda de acesso em ocasiões anteriores, relatar o fato e as circunstâncias.

Arquivos suspeitos - senhas

Nas situações de compartilhamento de senha com terceiros (NÃO RECOMENDADO EM HÍPOTESE NENHUMA), informe se houve acesso a sites suspeitos, instalação de softwares distintos ou cliques em links duvidosos.

Reportar diretamente

Quando os dados foram coletados durante o registro de ocorrência de forma integral, devem ser complementados durante a oitiva através de termo de declarações. Nesse caso, deve-se denunciar diretamente no provedor de e-mail ou na rede social a perda de acesso ou hackeamento e utilizar as opções para recuperação da conta.

Dicas de segurança

- Não compartilhe senhas.
- Use verificação de segunda etapa.
- Valha-se de senhas complexas e diferentes para cada aplicação.
- Não clique em links suspeitos.
- Utilize antivírus pagos.
- Evite acesso a sites nocivos.
- Mantenha os programas atualizados.
- Não faça login numa aplicação utilizando as credenciais de outra.

CRIMES CIBERNÉTICOS

Sextorsão

Riscos do Compartilhamento de Conteúdo íntimo.

O criminoso, através da utilização de um perfil fake e farta engenharia social, faz a abordagem ao usuário de internet convencendo-o a enviar imagens ou vídeos íntimos. Posteriormente exige pagamento para a não divulgação.

Modus operandi

- Uso de redes sociais, voip, sites de relacionamento, etc.
- Perfis fakes com fotos atraentes.
- Solicitação de amizade na rede social e envio de imagens íntimas.
- Insinuação rápida para sexo virtual.

Ferramentas utilizadas

Softwares que simulam streaming de vídeo.

Uso de tradutores online.

Pagamento da extorsão com criptomoeda ou transferência internacional.

Como evitar

Não compartilhe conteúdo íntimo.

Bom senso e dupla verificação dos fatos antes de adicionar perfil desconhecido.

Bloqueie a webcam quando não estiver em utilização.

Proteja as informações pessoais.

Altere as configurações de privacidade nas redes sociais.

Caso seja a vítima

Procure a delegacia mais próxima.

Não pague os valores exigidos.

Forneça informações das contas utilizadas pelos criminosos.

Preserve o conteúdo das conversas.

Typosquatting

Registro de nomes de domínio semelhantes aos de marcas ou empresas conhecidas para alcance de usuários através de digitação errônea ou de clicks em sites falsos com aparência de oficiais.

Finalidades

- Monetização de páginas com publicidade.
- Compartilhamento de fake news.
- Venda de domínio ou redirecionamento de tráfego para concorrente.
- Links maliciosos para a prática de fraudes eletrônicas.

Exemplos

Site original: ***www.meusite.com.br***

Substituição: www.meusyte.com.br

Erro: www.meustie.com.br

Omissão: www.mesite.com.br

Hifenação: www.meu-site.com.br

Adição: www.meusites.com.br

Alteração de domínios de topo do código do país e/ou genérico: www.meusite.com.bs e www.meusite.net

Minimize os riscos

Utilize inteligência de fontes abertas para checar as notícias relacionadas com a URL digitada.

Consulte o WHOIS da página.

Instale extensões verificadoras.

Confira blacklist de domínios.

Cryptojacking

Mineração maliciosa de criptomoeda.

É a infecção de dispositivo informático através de malware ou script com a finalidade de fazer mineração maliciosa de criptomoedas. Essa ação pode ocorrer de várias formas, entre as quais links maliciosos, incorporação de um código javascript em sites de terceiros, extensões de navegadores, jogos, propagandas online, sites torrentes, etc.

A mineração de moedas virtuais exige maior capacidade de processamento do dispositivo informático e, consequentemente, maior consumo de energia elétrica.

O Criptojacking aumenta consideravelmente os valores das faturas mensais de energia pagas pela vítima. O criminoso transferirá para ela os custos dessa mineração.

TIPIFICAÇÃO

Furto mediante fraude – art. 155, §§ 3º e 4º, II, do Código Penal. O criminoso, utilizando de artifício fraudulento, subtrai coisa alheia

móvel (energia elétrica). Há, portanto, efetiva diminuição patrimonial da vítima, além do que a quantidade de alvos infectados e a reiteração da conduta delitiva afastam a aplicação do princípio da insignificância.

Defacement

Defacement ou pichação eletrônica é o ato de modificar ou danificar um site hospedado na internet com os mais diversos propósitos (ativista ou político, pessoal, ataques contra indivíduos ou empresas, etc.).

TIPIFICAÇÃO

Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública.

Demais casos (fato atípico)

Obs.1:	Não há previsão legal no art. 154-A para a alteração de conteúdo de site na internet.
Obs.2:	Alguns doutrinadores entendem que a conduta configuraria crime de dano previsto no art. 163 do Código Penal.
	Art. 266, § 1º, do Código Penal. Interromper serviço telemático ou de informação de utilidade pública, ou impedir ou dificultar-lhe o restabelecimento.
Pena:	detenção de um a três anos e multa. Projeto de Lei n. 3.357/2015.
Autoria:	Dep. Vicentinho Júnior - PSB/TO.
	Dispõe sobre o crime de invadir dispositivo informático sem a devida autorização, modificando conteúdo de sítio da internet.
Situação:	pautado no PLENÁRIO (março 2019).

Bolware, fraudes por alteração de boleto bancário

É o *malware* instalado no computador da vítima para a modificação dos dados de criação e pagamento de boleto bancário. Quando a vítima gera o documento para pagamento através de um computador infectado, o malware altera a linha digitável, fazendo com que os valores sejam repassados para a conta de terceiros, e não do verdadeiro cedente/ beneficiário.

Dicas de segurança

- Mantenha o antivírus e o sistema operacional atualizados.
- Evite abrir links de terceiros e anexos de e-mails de fontes desconhecidas.
- Observe todas as informações do boleto.
  OBS.: Dados sobre as instituições financeiras podem ser consultados através do site Busca Banco da **FEBRABAN (http://www.buscabanco.org.br/)**. O boleto deve ter nome e logomarca do banco emissor coincidentes. A linha digitável deve conter agência, código cedente e nosso número, independentemente do banco emissor do boleto. O número do banco e os três primeiros caracteres da linha digitável devem ser iguais.

Exposição de intimidade sexual é crime

A exposição da intimidade sexual é infração penal. Fotografar, filmar, registrar, fazer montagens ou compartilhar conteúdo íntimo sem autorização dos participantes são crimes tipificados no Código Penal.

Registro não autorizado da intimidade sexual. Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de

nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes. Pena - detenção de seis meses a um ano e multa.

Montagem em cena de nudez, ato sexual ou libidinoso. Art. 216-B, parágrafo único. Realizar montagem em fotografia, vídeo áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. Pena - detenção de seis meses a um ano e multa.

Divulgação de cena de sexo ou de pornografia. Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio, inclusive por meio de comunicação de massa ou sistema de informática ou telemática sem o consentimento da vítima, cena de sexo, nudez ou pornografia. Pena - reclusão de um a cinco anos.

Crimes cibernéticos praticados contra crianças e menores de idade

Obrigatoriedade na Remoção de Imagens ou Vídeos de Abuso e Exploração Sexual Infantojuvenil

Os representantes legais das redes sociais, aplicativos de mensageria, serviços de compartilhamento de vídeos, sites e blogs devem, a partir do recebimento da notificação, excluir de suas plataformas todo e qualquer conteúdo que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

SANÇÕES PARA O DESCUMPRIMENTO

Caso não desabilite o acesso ao conteúdo ilícito, o responsável pelo serviço responderá por crime previsto no art. 241-A do Estatuto da Criança e do Adolescente, com pena de reclusão de três a seis anos e multa.

Fraude por internet banking

CONTEXTUALIZAÇÃO

Nessa modalidade criminosa ocorre a burla do sistema de proteção e de vigilância do banco com a subtração de valores mantidos sob a guarda deste. Posteriormente, sem qualquer tipo de consentimento da vítima, o infrator realiza transferências bancárias para terceiros, executa compras online e efetua o pagamento de impostos e taxas. A consumação do crime ocorre com a subtração dos valores da conta da vítima.

TIPIFICAÇÃO PENAL

Crime de furto qualificado pela fraude. Art. 155 § 4º, ll. Pena - reclusão de dois a oito anos e multa.

Fraude eletrônica por RAT bancário

O RAT bancário ou "Trojan de Acesso Remoto" é o malware utilizado pelos criminosos para assumir o controle do computador da ví-

tima, subtrair credenciais de acesso de internet banking e desviar valores de contas sem conhecimento dela. Na prática, executa ações de programas legítimos e age como se estivesse utilizando fisicamente o computador da vítima.

Modus operandi

O criminoso envia o RAT bancário através de:
Anexos de e-mail
Links maliciosos
Programas com malwares ocultos baixados pelos usuários

Precauções

Mantenha o antivírus e sistema operacional atualizados
Evite abrir anexos de e-mails de fontes não confiáveis
Desative portas não utilizadas
O firewall deve estar ativado e configurado adequadamente

Golpes no Whatsapp e fraudes eletrônicas - Prescindibilidade de ordem judicial para o fornecimento de dados pelas instituições financeiras

CONTEXTUALIZAÇÃO

O fornecimento de contas bancárias para o recebimento de valores subtraídos é uma das peculiaridades dos crimes cometidos online

(clonagem de WhatsApp, fraudes eletrônicas, estelionato, furto mediante fraude, etc.).

Além dos dados cadastrais, a autoridade policial poderá requisitar, independentemente de ordem judicial, as informações sobre operações que envolvam os recursos provenientes dessa prática criminosa.

Assim, toda e qualquer operação ilícita decorrente de valor subtraído ou obtido de forma indevida deverá ser fornecida para instruir investigação policial em andamento, sem haver necessidade de representação pela quebra de sigilo bancário.

FUNDAMENTAÇÃO LEGAL

Lei Complementar n. 105, de 10 de janeiro de 2001. Art. 1º, § 3º: Não constitui violação do dever de sigilo: IV A comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa.

Referências

BARRETO, Alessandro Gonçalves

Cybercards – Meio Cibernético: Orientações Práticas.,. São Paulo, 2019 por Alessandro Gonçalves Barreto.

Investigação Criminal: provas by Cristiano Ritta, Emerson Wendt, Valquiria Wendt, Bolivar Llantada, eAlessandro Barreto

MERCÊS, Fernando. **O que fazer antes que seu celular seja roubado.** Mente Binária, 14 maio 2019. Disponível em: https://www.mentebinaria.com.br/

Leituras recomendadas

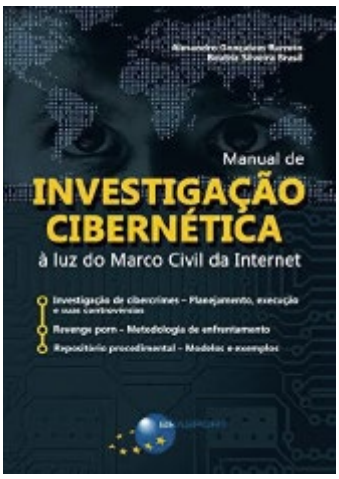
MITNICK, Kevin. **PROOF** – Segurança da Informação, 2016. Vídeo (7 min 39 s). Disponível em: https://www.youtube.com/watch?v=1DUpheNCkEQ. Acesso em: 6 fev. 2020.

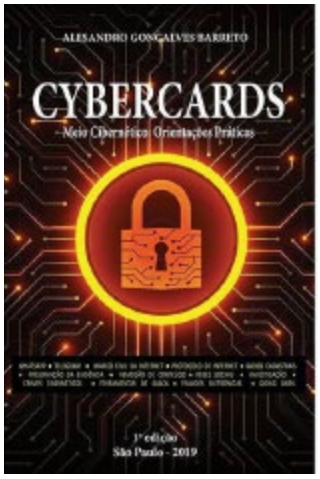
NATIONAL CYBER SECURITY CENTRE. **The top 100,000 passwords from Troy Hunt's have I been Pwned.** [S.l.], 2019. Disponível em: https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt. Acesso em: 6 fev. 2020.

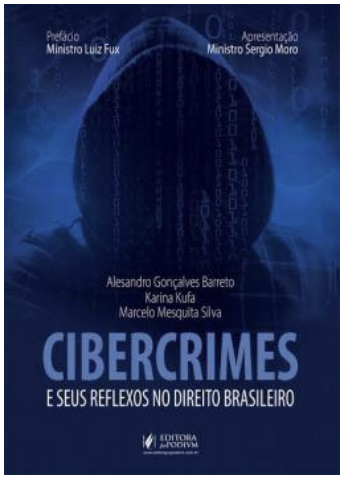
SILVA, Rafael Rodrigues da. Órgão britânico revela lista com as senhas mais utilizadas no mundo. **HostGator**, 22 abr. 2019. Disponível em: https://canaltech.com.br/seguranca/orgao-britanico-revela-lista-com-as-

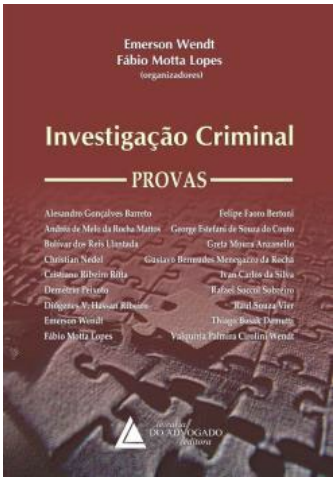
-senhas-mais-utilizadas-no-mundo-137683/. Acesso em: 6 fev. 2020.

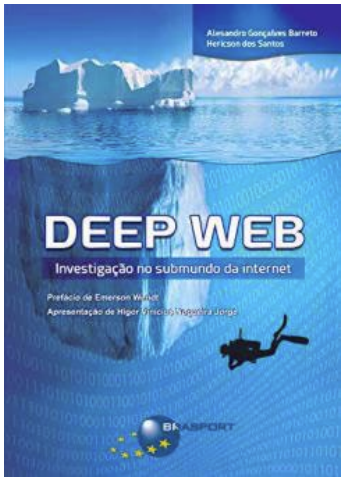
TRIBUNAL DE JUSTIÇA DE SANTA CATARINA. **Resolução GP N. 10 de 21 de março de 2018.** Cria o Núcleo de Inteligência e Segurança Institucional no Tribunal de Justiça e dá outras providências. Florianópolis, 26 mar. 2018. Disponível em: http://busca.tjsc.jus.br/buscatextual/integra.do?cdSistema=1&cdDocumento=171433&cdCategoria=1&q=&frase=&excluir=&qualquer=&prox1=&prox2=&proxc=. Acesso em: 6 fev. 2020.

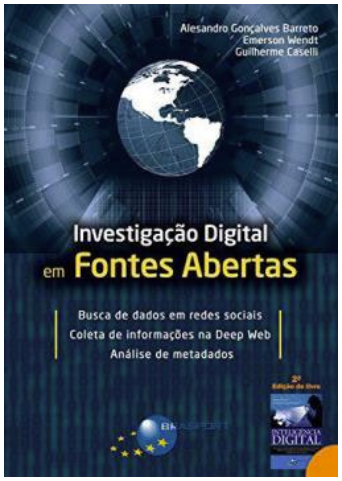












CARTILHA DE SEGURANÇA CIBERNÉTICA

Prevenção e orientações contra crimes cibernéticos

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
de Santa Catarina
Gabinete da Presidência
Núcleo de Inteligência e Segurança Institucional