

CRIMES CIBERNÉTICOS:

OS PRINCIPAIS RISCOS E TÉCNICAS BÁSICAS DE PREVENÇÃO



POLÍCIA CIVIL DE MINAS GERAIS
ACADEMIA DE POLÍCIA CIVIL DE MINAS GERAIS

CRIMES CIBERNÉTICOS:
OS PRINCIPAIS RISCOS E TÉCNICAS BÁSICAS DE PREVENÇÃO

Administração: Dra. Cinara Maria Moreira Liberal
Belo Horizonte – 2020

CRIMES CIBERNÉTICOS:
OS PRINCIPAIS RISCOS E TÉCNICAS BÁSICAS DE PREVENÇÃO

Coordenação Geral

Dra. Cinara Maria Moreira Liberal

Subcoordenação Geral

Dr. Marcelo Carvalho Ferreira

Coordenação Didático-Pedagógica

Rita Rosa Nobre Mizerani

Coordenação Técnica

Dra. Elisabeth Terezinha de Oliveira Dinardo Abreu

Conceudista:

Dr. Guilherme da Costa Oliveira Santos

Larissa Dias Paranhos

Samuel Passos Moreira

Produção do Material:

Polícia Civil de Minas Gerais

Revisão e Edição:

Divisão Psicopedagógica – Academia de Polícia Civil de Minas Gerais

Reprodução Proibida

SUMÁRIO

1 OUTROS RISCOS NO USO DA INTERNET	3
1.1 Ataques na internet	3
1.2 Códigos Maliciosos (malwares).....	5
1.3 Spam	7
2 O USO SEGURO DA INTERNET E OS MECANISMOS DE SEGURANÇA.....	9
3 REFERÊNCIAS	14

1 OUTROS RISCOS NO USO DA INTERNET

Além dos vários golpes virtuais apresentados no Capítulo 3, a internet, como destacado no início deste curso, apresenta outros riscos, que incluem os chamados códigos maliciosos, ataques e spams e sobre eles falaremos aqui.

Não é objetivo deste curso aprofundar nesses temas, mas, apenas, fazer breves explanações, para conscientizar todos acerca da existência de outros riscos no meio virtual.

1.1 Ataques na internet

Assim como os vários golpes, ataques na internet podem ter como alvos serviços, computadores ou redes acessíveis via internet.

Para obter sucesso, os atacantes usam diversas técnicas e têm objetivos diferentes, tais como a **demonstração de poder** (mostrar para uma empresa que ela pode ser invadida); **prestígio** (vangloriar-se ante outros atacantes); **motivações financeiras** (obter informações confidenciais para aplicar outros golpes); **ideológicas** (invadir um site que divulga ideias contrárias às do atacante), **comerciais** (tornar o site de uma empresa indisponível para impedir o acesso dos seus clientes, comprometendo a sua reputação) (CERT.br, 2017).



Dentre as técnicas mais utilizadas por atacantes, seguem abaixo as principais:

A. Exploração de vulnerabilidades

É quando o atacante, aproveitando-se de uma vulnerabilidade (má configuração de programas, serviços ou equipamentos de rede, por exemplo), tenta executar ações maliciosas, como invadir o sistema ou acessar informações confidenciais.

B. Varredura em redes (*Scan*)

Técnica usada para fazer buscas minuciosas em redes com o intuito de identificar computadores ativos e coletar informações sobre eles (como quais os programas instalados), associando possíveis vulnerabilidades existentes para, depois, explorá-las. Um exemplo é a propagação de códigos maliciosos (CERT.br, 2017).

C. Falsificação de e-mail (E-mail *spoofing*)

Trata-se de uma técnica para alterar os campos do cabeçalho, de modo que a vítima acredite que ele foi enviado por determinada pessoa (ou empresa), quando, na

verdade, a origem é outra. O objetivo é convencer a vítima de que o atacante é algo ou alguém que ele não é (OLIVEIRA, 2003). Um exemplo são os falsos e-mails de bancos solicitando que você clique em um *link* e execute um arquivo anexo. Outra situação que pode ocorrer é você receber um e-mail aparentemente enviado por você mesmo, sem que você jamais tenha feito isso.



D. Interceptação de tráfego

É a técnica de monitorar os dados que trafegam em redes de computadores, utilizando, para tanto, programas chamados de *sniffers* (OLIVEIRA, 2003). O objetivo, por exemplo, pode ser roubar senhas ou números de cartões de crédito.

E. Força bruta (*Brute force*)

Trata-se da técnica usada para adivinhar, por tentativas e erros, o nome de um usuário e senha e, desse modo, executar processos e acessar sites, computadores ou serviços em nome e com os mesmos privilégios deste usuário (CERT.br, 2017). Assim, por exemplo, se o atacante sabe o login e a senha do seu e-mail, ele pode ver todas as suas mensagens e contatos e, ainda, enviar mensagens em seu nome. No caso de uma rede social, se o atacante conhece o seu usuário e senha, ele pode enviar mensagens para os seus seguidores contendo códigos maliciosos.

F. Desfiguração de página (*Defacement ou Deface*)

Consiste em modificar o conteúdo ou a estética de uma página da web. Essa forma de ataque é muito usada em cunho ativista ou político, em sites de ONGs e instituições públicas ou privadas, com o objetivo de degradar ou desmoralizar informações ali transmitidas (CANALTECH, 2020). Esse ataque é comparado a uma pichação de muros ou paredes.

G. Negação de serviço (*DoS*)

O *DoS* (*Denial of Service*) é uma técnica em que o atacante usa um terminal para deixar indisponível um serviço, terminal ou rede conectada à internet. Quando um conjunto de terminais é utilizado no ataque, fala-se em negação de serviço distribuído ou *DDoS* (*Distributed Denial of Service*) (OLIVEIRA, 2003). O objetivo destes ataques não é invadir ou coletar informações, mas sim esgotar os recursos e provocar indisponibilidades ao alvo. Quando o ataque tem sucesso, as pessoas que dependem daqueles recursos afetados são prejudicadas, pois ficam impossibilitadas de acessar ou realizar as operações desejadas (CERT.br, 2017), como utilizar o site de um banco, por exemplo.

A melhor forma de um usuário se prevenir contra esses ataques é **proteger os seus dados**, utilizar os **mecanismos de proteção** disponíveis, incluindo a criação de senhas “fortes” e instalar um bom antivírus, além de manter o seu terminal atualizado e a salvo de códigos maliciosos.

Mas, o que são os **CÓDIGOS MALICIOSOS?**

1.2 Códigos Maliciosos (malwares)

Códigos maliciosos (ou *malwares*) são programas criados para **executar ações danosas** em um terminal e, depois de instalados, passam a ter **acesso a todos os dados ali armazenados** (ROCHA, 2015).



O objetivo de uma pessoa que desenvolve um código malicioso pode ser **obter vantagens financeiras, coletar informações sigilosas, autopromover-se** e, até mesmo, **praticar vandalismo**. O uso desses *malwares* pode estar associado à prática de golpes e ataques (como os já estudados) ou à disseminação de *spams* (CERT.br, 2017).

Dentre os tipos de códigos maliciosos existentes, podem-se citar os seguintes:



A. Vírus

É um programa (ou parte de um programa) com instruções “maldosas” para alterar dados ou sistemas, destruir, alterar arquivos e programas, ou executar funções inesperadas em um sistema computacional ou em dispositivo informatizado (JESUS; MILAGRE, 2016).

Para ser ativado (e realizar alguma ação), não basta que você tenha o vírus no terminal; é preciso executar o programa ou arquivo que o contém. Um exemplo de vírus são arquivos infectados enviados por e-mails, que, ao serem abertos, infectam outros arquivos e programas e envia cópias de si mesmo para os e-mails encontrados na lista de contatos (CERT.br, 2017).

B. Worm

É um tipo de código malicioso mais perigoso que um vírus comum, pois ele se propaga rapidamente e isso ocorre sem controle da vítima, isto é, não exige que a vítima abra o arquivo infectado ou execute o programa. Assim que o *worm* contamina um terminal, o programa malicioso cria cópias de si mesmo em vários locais do sistema e alastrá-se para outros terminais, por meio da internet, de mensagens, conexões locais, dispositivos USB ou arquivos. Em geral, o objetivo do criminoso é roubar dados do usuário ou de empresas e podem ser transmitidos através de arquivos corrompidos ao acessar uma página suspeita (STIVANI, 2018).

C. Bot e botnet

Bot é um programa com mecanismos de comunicação com o invasor, que permitem que ele seja controlado de forma remota. O processo de infecção e propagação é bastante similar ao do *worm*, pois pode se propagar automaticamente, explorando vulnerabilidades de programas já instalados em terminais. O equipamento infectado se torna um “zumbi” e pode receber instruções maliciosas para, por exemplo, furtar dados do terminal. A *Botnet*, por sua vez, é uma rede de computadores composta por vários *bots* prontos para receber comandos maliciosos (BARÃO; VILAR, 2016).

D. Spyware

É um *malware* espião criado para monitorar as atividades *online*, o histórico e os dados pessoais, a fim de repassar informações para terceiros. Esse tipo de código malicioso é um dos mais perigosos que existe, pois ele busca informações sigilosas que podem ser usadas para variados fins e, até mesmo, o furto de senhas pessoais, informações bancárias ou de cartões de crédito (ARAÚJO, 2019).

E. Backdoor

É um tipo de código malicioso que permite o retorno do invasor a um terminal comprometido, através da inclusão de serviços criados ou modificados para este fim (JESUS; MILAGRE, 2016). Trata-se de uma porta de acesso criada pelo criminoso no sistema do terminal da vítima a partir da instalação não autorizada de um programa e que permite o seu retorno para ações futuras, através de acessos remotos. Geralmente, é instalado a partir de uma falha de segurança e colocado de forma a não ser notado pela vítima.

F. Cavalo de Troia (*Trojan*)

É um programa que, além de executar as funções para as quais foi aparentemente projetado, executa outras funções, em regra, maliciosas, e sem que o usuário tome conhecimento. Exemplos de *trojans* são programas que você recebe ou obtém em sites e que aparecem ser apenas cartões virtuais animados, álbuns de fotografias, *games* e protetores de tela, etc. Estes programas, normalmente, são formados por um só arquivo e precisam ser executados para que sejam instalados no terminal (CERT.br, 2017). Na maioria das vezes, esses *malwares* são usados para obter informações de outros dispositivos ou executar operações indevidas.



G. Rootkit

É um conjunto de técnicas e programas, na maioria das vezes maliciosos, criados para esconder ou camuflar e assegurar a presença de um invasor ou outros códigos maliciosos em um terminal comprometido. A título de exemplo, um *rootkit* pode comprometer um programa navegador, que, quando é executado, também aciona uma função que abre uma porta da máquina (*backdoor*) para ser acessada por outro invasor atacante (JESUS; MILAGRE, 2016).

Para manter o seu equipamento a salvo da ação dos *malwares*, é essencial adotar algumas medidas preventivas, dentre as quais estão sempre atualizar os programas instalados e utilizar mecanismos de segurança, como *antimalwares* e *firewall* pessoal, os quais serão apresentados no próximo capítulo.

Por fim, para facilitar o entendimento de como os equipamentos são infectados por *malwares*; a forma como eles são instalados; como eles se propagam; e, as mais comuns ações maliciosas por eles executadas, segue um **QUADRO-RESUMO**:

	Vírus	Worm	Bot	Trojan	Spyware	Backdoor	Rootkit
Como é obtido:							
Recebido automaticamente pela rede		✓	✓				
Recebido por e-mail	✓	✓	✓	✓	✓		
Baixado de sites na Internet	✓	✓	✓	✓	✓		
Compartilhamento de arquivos	✓	✓	✓	✓	✓		
Uso de mídias removíveis infectadas	✓	✓	✓	✓	✓		
Redes sociais	✓	✓	✓	✓	✓		
Mensagens instantâneas	✓	✓	✓	✓	✓		
Inserido por um invasor		✓	✓	✓	✓	✓	✓
Ação de outro código malicioso		✓	✓	✓	✓	✓	✓
Como ocorre a instalação:							
Execução de um arquivo infectado	✓						
Execução explícita do código malicioso		✓	✓	✓	✓		
Via execução de outro código malicioso						✓	✓
Exploração de vulnerabilidades		✓	✓		✓	✓	✓
Como se propaga:							
Insere cópia de si próprio em arquivos	✓						
Envia cópia de si próprio automaticamente pela rede		✓	✓				
Envia cópia de si próprio automaticamente por e-mail		✓	✓				
Não se propaga				✓	✓	✓	✓
Ações maliciosas mais comuns:							
Altera e/ou remove arquivos	✓			✓			✓
Consume grande quantidade de recursos		✓	✓				
Furta informações sensíveis			✓	✓	✓		
Instala outros códigos maliciosos	✓	✓	✓				✓
Possibilita o retorno do invasor						✓	✓
Envia spam e phishing				✓			
Desfere ataques na Internet		✓	✓				
Procura se manter escondido	✓				✓	✓	✓

Fonte: CERT.br. Cartilha de Segurança para a Internet. (2017).

1.3 Spam

O *spam* é uma prática que afeta 100% dos usuários da internet e, infelizmente, **não há como evitar**, apenas minimizar os danos que eles podem causar. Traduzindo-se de forma literal para o português, *spam* (*Sending and Posting Advertisement in Mass*) significa “**“enviar e postar publicidade em massa”**” (ALENCAR, 2016).



Na prática, o *spam* é a mensagem eletrônica enviada por *spammers* (pessoas responsáveis pelo envio) para o usuário sem sua permissão ou sem o seu desejo em recebê-lo. Normalmente, os *spams* têm cunho **comercial** e são enviados por e-mail (aquele propagandas indesejadas de lojas e produtos), mas também podem circular em redes sociais ou comentários de blogs e ter objetivo criminoso (ALENCAR, 2016).

Os *spams* associam-se diretamente a ataques à segurança da internet e do usuário e constituem um dos grandes responsáveis pela proliferação de *malwares*, disseminação de golpes e venda ilegal de produtos.

Além disso, dentre os vários problemas causados por *spams*, estão **a perda de mensagens importantes**, pois devido ao número de *spams* enviados, é possível que você deixe de ler uma mensagem de seu interesse ou acabe apagando-a por engano; **o recebimento de conteúdos impróprios ou ofensivos**, uma vez que *spams* são enviados para um conjunto aleatório de e-mails e nem todos os usuários classificam os assuntos como adequados; **o gasto desnecessário de tempo**, sobretudo para apagar *spams*; **o não recebimento de e-mails importantes**, pois se o seu serviço de e-mail tem limite no tamanho da caixa postal, ela pode se encher rapidamente e você acabar não recebendo um e-mail relevante, entre outros infortúnios (CERT.br, 2017).

Algumas das principais características¹ dos *spams* são:

Apresentam cabeçalho suspeito: o cabeçalho do e-mail aparece incompleto, por exemplo, os campos de remetente e/ou destinatário aparecem vazios ou com apelidos/nomes genéricos, como "amigo@" e "suporte@".

Apresentam no campo Assunto (Subject) palavras com grafia errada ou suspeita: a maioria dos filtros *antispam* utiliza o conteúdo deste campo para barrar e-mails com assuntos considerados suspeitos. No entanto, os *spammers* adaptam-se e tentam enganar os filtros colocando neste campo conteúdos enganosos, como "vi@gra" (em vez de "viagra").

Apresentam no campo Assunto textos alarmantes ou vagos: na tentativa de confundir os filtros *antispam* e de atrair a atenção dos usuários, os *spammers* costumam colocar textos alarmantes, atraentes ou vagos demais, como "Sua senha está inválida", "A informação que você pediu" e "Parabéns".

Oferecem opção de remoção da lista de divulgação: alguns *spams* tentam justificar o abuso, alegando que é possível sair da lista de divulgação, clicando no endereço anexo ao e-mail. Este artifício, porém, além de não retirar o seu endereço de e-mail da lista, também serve para validar que ele realmente existe e que é lido por alguém [...] (CERT.br, 2017).

Há medidas que podem ajudar você a reduzir a quantidade de *spams* recebidos, como, por exemplo: **1)** Filtrar as mensagens indesejadas, por meio de programas instalados em seu equipamento e de sistemas integrados a Webmails e leitores de e-mails; **2)** Colocar as mensagens classificadas como *spam* em quarentena através de filtros; **3)** Ter cuidado ao fornecer seu endereço de e-mail, pois você pode estar abrindo uma porta para receber *spams*; **4)** Atentar-se para opções pré-selecionadas. Em alguns formulários ou cadastros preenchidos pela internet, há a pergunta se você quer receber e-mails, por exemplo, sobre promoções.

¹ Nem todas essas características podem estar presentes ao mesmo tempo em um mesmo *spam*. Além disso, é possível que haja *spams* que não atendam às propriedades citadas, podendo, eventualmente, ser um novo tipo (CERT.br, 2017).

2 O USO SEGURO DA INTERNET E OS MECANISMOS DE SEGURANÇA

O primeiro grande passo para se prevenir dos riscos existentes na internet é ter em mente de que, nela, **NADA É “VIRTUAL”**. Tudo aquilo que acontece na internet ou é realizado por meio dela é **real**: os dados são reais e as empresas e pessoas que interagem com você são as mesmas com que você interage aqui fora. Portanto, os riscos aos quais você está exposto na web são os mesmos que você presencia no seu dia a dia e os golpes cibernéticos são bastante similares àqueles que ocorrem na rua ou por telefone (CERT.br, 2017).

Por este motivo, é preciso que você tenha na internet os mesmos cuidados que adota no seu cotidiano, tais como: comprar apenas em lojas confiáveis; ter atenção com as pessoas ao seu redor quando vai ao banco; não fornecer a senha dos seus cartões para ninguém; não deixar a porta da sua casa aberta; não deixar que crianças e adolescentes falem com estranhos ou vá a lugares perigosos sozinhos; contratar sistemas de monitoramento de câmeras e alarme para proteger a sua casa.

De maneira geral, para minimizar os riscos aos quais podemos ser expostos na internet, a adoção de alguns mecanismos de segurança se faz necessária. Esses



mecanismos contribuem, por exemplo, para identificar uma pessoa, empresa ou programa; ativar fatores de autenticação (assegurando que determinada pessoa é quem ela diz ser); autorizar a realização de certas ações; e, proteger informações contra alterações e acessos não autorizados.

Dentre os diversos **mecanismos de segurança** existentes, podemos destacar:

A. Política de segurança

São as regras sobre os direitos e responsabilidades de cada uma das partes envolvidas (usuários e instituições, por exemplo) no tocante à segurança dos recursos computacionais utilizados e as sanções às quais estão sujeitos, caso não as cumpram. A política de segurança pode tratar de **senhas** (número de caracteres, composição e periodicidade de troca), **privacidade** (define regras de tratamentos de informações pessoais), **confidencialidade** (define se as informações podem ser divulgadas a terceiros) e outros assuntos importantes. Esteja sempre atento à política de segurança dos sites acessados e serviços contratados na internet, bem como às suas possíveis alterações ao longo do tempo, para não ser pego de surpresa (CERT.br, 2017).

B. Notificação de incidentes e abusos

O incidente de segurança é todo evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas de computação ou redes de computadores, tais como a tentativa de usar ou acessar sem autorização sistemas ou dados; a tentativa de indisponibilizar serviços; modificar sistemas e desrespeitar a política de segurança de uma instituição (CERT.br, 2017). É de suma importância notificar a instituição ou pessoa responsável sempre que detectada a existência desses incidentes ou abusos.



De modo geral, a lista de pessoas/entidades a serem notificadas inclui: os responsáveis pelo computador que originou a atividade, os responsáveis pela rede que originou o incidente (incluindo o grupo de segurança e abusos, se existir um para aquela rede) e o grupo de segurança e abusos da rede a qual você está conectado (seja um provedor, empresa, universidade ou outro tipo de instituição) (CERT.br, 2017).

A notificação de incidentes é de suma importância para a sua proteção na web e contribui, também, para a segurança de toda a Internet, além de ajudar outras pessoas a detectarem problemas, como, por exemplo, computadores contaminados, falhas de configuração e transgressões a políticas de segurança.



C. Contas e senhas

Atualmente, o mecanismo de autenticação mais utilizado para controlar o acesso a sites e serviços ofertados na web é o uso de contas e senhas, por meio das quais os vários sistemas conseguem identificar que é você quem está realizando o acesso e definir as ações que você pode executar.

A proteção de uma senha é essencial para uma navegação segura e essa segurança é colocada em risco (podendo facilitar a identificação da senha), por exemplo, ao **utilizar um equipamento infectado**; **acessar um site falso**; ser enganado por **técnicas de engenharia social**; através da **captura do movimento dos dedos no teclado ou dos cliques do mouse em teclados virtuais**; ou, até mesmo, pelo simples **acesso a arquivos onde ela esteja armazenada**.

Em determinadas situações, suas senhas devem ser alteradas **IMEDIATAMENTE**, como, por exemplo, se o seu equipamento onde elas estão armazenadas for roubado; se você utilizar um mesmo padrão de senhas para acessar determinados sites e desconfiar que alguma delas foi descoberta; sempre que adquirir equipamentos acessíveis pela rede, como um roteador e dispositivos bluetooth, que possuem senhas-padrão.

Além da proteção básica das suas senhas, deve-se saber criar senhas “**FORTES**”.

FIQUE SABENDO:

Para criar senhas “**FORTES**”, 3 dicas são essenciais:

- 1^a.** Use **números aleatórios** (quanto mais ao acaso forem os números melhor).
- 2^a.** Abuse da **grande quantidade de caracteres** (quanto mais longa for a senha mais difícil será descobri-la).
- 3^a.** Escolha **diferentes tipos de caracteres** (quanto mais “bagunçada” for a senha mais difícil será descobri-la).

D. Criptografia

É a arte da escrita secreta, isto é, uma técnica para codificar dados que, depois, serão decodificados pela decriptografia. Existem criptografias fracas, que são fáceis de decifrar, e outras fortes, que são difíceis e, num primeiro momento, impossíveis de ler (OLIVEIRA, 2003). Em regra, a criptografia é usada para que você proteja dados contra acessos indevidos, sejam aqueles que precisam ser transmitidos via internet ou armazenados em um equipamento.



E. Cópias de segurança (*Backup*)

Uma medida preventiva que deve se tornar rotina para o usuário da internet é a cópia de segurança, isto é, o *backup*. Certamente, eventos indesejados podem ocorrer, como o computador queimar, o celular ser roubado, você se esquecer de onde guardou um pendrive e, com isso, perder informações importantes (OLIVEIRA, 2003).

Os *backups* podem ser armazenados em mídias (como pendrives e HDs externos) ou serem armazenados em nuvem (como os conhecidos Google Drive e iCloud). A periodicidade com que você deve fazer o *backup* pode variar de acordo com a frequência em que você altera os dados a serem armazenados. É sempre importante manter as cópias de segurança atualizadas e em locais seguros.

F. Ferramentas *antimalware*

São softwares que buscam detectar e, então, anular ou extrair códigos maliciosos de um equipamento (computador, tablet, celular). Antivírus, *Antispyware*, *Antirootkit* e *Antitrojan* são exemplos de ferramentas dessa natureza (ROCHA, 2015). Há, também, ferramentas específicas para cada um dos tipos de códigos maliciosos.

G. Firewall pessoal

Em rede de computadores, o *firewall* funciona como uma “parede de fogo”; é um recurso responsável por filtrar toda a informação que chega a uma rede, garantindo sua segurança. Na hipótese de o filtro considerar algum dado malicioso, ele não poderá ser acessado e será bloqueado automaticamente (COSTA, 2020).



O firewall pessoal garante um nível de segurança a mais para o equipamento, com o bloqueio (e registro) de tentativas de acessos não autorizadas, incluindo invasões e exploração de vulnerabilidades existentes.

Além de outras funções, o firewall pessoal também pode evitar que um *malware* já existente no dispositivo se propague.

H. Filtro *antispam*

Normalmente, já vem integrado a grande parte dos Webmails e programas leitores de e-mails e permite separar os e-mails desejados daqueles indesejados (*spams*) (CERT.br, 2017).

Diante do exposto, verifica-se que existem vários mecanismos de segurança para você se proteger ao realizar o acesso à internet. Além deles, outros cuidados podem ser adotados para garantir um acesso seguro à web. Vejamos alguns:

Ao usar **NAVEGADORES WEB**:

- A.** Mantenha-o atualizado e ative a configuração para fazer atualizações automaticamente, inclusive de complementos que estejam instalados.
- B.** Seja cuidadoso ao usar *cookies* caso deseje ter mais privacidade.
- C.** Se optar por permitir que o navegador grave as suas senhas, tenha a certeza de cadastrar uma chave mestra e de jamais esquecê-la.
- D.** Mantenha seu computador seguro (CERT.br, 2017).



Ao acessar **WEBMAILS**:

- 1)** Cuidado para não ser vítima de phishing (golpe para obter os seus dados confidenciais). Digite a URL diretamente no navegador e tenha cuidado quando clicar em links recebidos por mensagens eletrônicas.
- 2)** Crie senhas “fortes” para acessar o seu Webmail.
- 3)** Configure opções de recuperação de senha como um e-mail alternativo ou um número de celular.
- 4)** Evite acessar seu Webmail em terminais de terceiros e, se realmente for necessário, ative o modo de navegação anônima.
- 5)** Certifique-se de utilizar conexões seguras. Evite redes Wi-Fi públicas.
- 6)** Mantenha o seu dispositivo seguro (CERT.br, 2017).

Ao realizar **TRANSAÇÕES BANCÁRIAS** e acessar **SITES DE INTERNET BANKING**:

- A.** Certifique-se de utilizar uma conexão segura e a procedência do site.
- B.** Digite o endereço diretamente no navegador web; nunca clique em links existentes em uma página ou mensagem.
- C.** Nunca forneça senhas ou dados pessoais a terceiros, principalmente por telefone.
- D.** Desconsidere mensagens de bancos com os quais você não tem relação, especialmente quando solicitarem seus dados pessoais ou a instalação de módulos de segurança.
- E.** Na dúvida, sempre entre em contato com a Central de Relacionamento do seu banco ou diretamente com o seu gerente.
- F.** Não faça transações bancárias a partir de equipamentos de terceiros ou Wi-Fi públicas.
- G.** Verifique, regularmente, o extrato da sua conta e do seu cartão de crédito e, se detectar um lançamento suspeito, entre em contato imediatamente com o seu banco ou com a operadora do seu cartão.
- H.** Antes de instalar qualquer módulo de segurança, verifique se o autor do módulo é realmente o seu banco.
- I.** Mantenha o seu equipamento sempre seguro (CERT.br, 2017).

Ao utilizar o **SEU CELULAR**:

- A.** Tenha guardado marca, modelo, IMEI e número de série do seu aparelho (geralmente essas informações estão disponíveis na caixa dele). Anote também o PIN e PUK do chip (vem no cartão entregue pela operadora).
- B.** 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.
- C.** Utilize a autenticação de dois fatores em todas as suas contas de redes sociais e serviços de internet (Facebook, Instagram, Twitter, Gmail, Icloud, etc.).
- D.** Habilite a ‘Confirmação em duas etapas’ no aplicativo do WhatsApp.
- E.** Sempre habilite o Touch ID (leitor de impressão digital), reconhecimento facial ou senha para todos os aplicativos que suportam.
- F.** 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.
- G.** 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 recentes códigos, mensagens e e-mails recebidos (MERCÊS, 2019).

E se eu **PERDER** meu celular ou ele for **ROUBADO / FURTADO?**



- 1)** Ligue para a sua operadora e informe o ocorrido. Ela irá bloquear o chip.
- 2)** Cancele os seus cartões de crédito que estejam vinculados ao aparelho (Apple Pay, Android Pay, Samsung Pay, dentre outros). Há casos em que ladrões utilizam Apple Pay e similares para fazer compras ou pedir comida em aplicativos como iFood e Uber Eats.
- 3)** Faça um boletim de ocorrência na Delegacia mais próxima. 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 (ex.: Gmail, Facebook, Instagram, Twitter, Spotify, etc.).
- 5)** Programe para deletar os dados pelo site do fabricante (Google, Apple, etc.) (MERCÊS, 2019).

Essas são apenas algumas dicas de segurança que você **DEVE** adotar no seu dia a dia. **O importante é manter-se sempre informado**; novas formas de golpes podem surgir e você pode antecipar a sua prevenção.

Se você tiver dúvidas ou precisar de ajuda, **procure a Delegacia de Polícia mais próxima de você**.

3 REFERÊNCIAS

ALENCAR, Felipe. O que é spam? **TechTudo**, 25 de julho de 2016. Disponível em: <<https://www.techtudo.com.br/noticias/noticia/2016/07/o-que-e-spam.html>>. Acesso em: 1º jul. 2020.

ALVES, Paulo. Golpe do boleto falso: sete dicas para não cair em armadilhas. **TechTudo**, 20 de outubro de 2019. Disponível em: <<https://www.techtudo.com.br/listas/2019/10/golpe-do-boleto-falso-sete-dicas-para-nao-cair-em-armadilhas.ghtml>>. Acesso em: 1º jul. 2020.

ARAÚJO, Giulia. O que é spyware? Entenda como age o 'app espião' e veja como se proteger. **TechTudo**, 07 de julho de 2019. Disponível em: <<https://www.techtudo.com.br/noticias/2019/07/o-que-e-spyware-entenda-como-age-o-app-espiao-e-veja-como-se-protoger.ghtml>>. Acesso em: 02 jul. 2020.

BARÃO, Rafael Eduardo; VILAR, Gustavo Pinto. Exames em *malwares*. In: VELHO, Jesus Antônio (org.). **Tratado de Computação Forense**. Campinas, SP: Millennium, 2016. p.409-446.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 02 jul. 2020.

_____. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 02 jul. 2020.

CANALTECH. **O que é defacement ou deface?**. Disponível em: <<https://canaltech.com.br/produtos/O-que-e-defacement-ou-deface/>>. Acesso em: 02 jul. 2020.

CARDOSO, Pedro. O que é Ransomware? **TechTudo**, 17 de maio de 2017. Disponível em: <<https://www.techtudo.com.br/noticias/noticia/2016/06/o-que-e-ransomware.html>>. Acesso em: 1º jul. 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para a Internet**. Disponível em: <<https://cartilha.cert.br/seguranca/>>. Acesso em: 30 jun. 2020.

COELHO, Taysa. O que é sextorsão? Entenda o crime que envolve imagens de teor sexual. **TechTudo**, 03 de dezembro de 2018. Disponível em: <<https://www.techtudo.com.br/noticias/2018/12/o-que-e-sextorsao-entenda-o-crime-que-envolve-imagens-de-teor-sexual.ghtml>>. Acesso em: 30 jun. 2020.

COSTA, Matheus Bigogno. O que é Firewall. **CanalTech**, 18 de fevereiro de 2020. Disponível em: <<https://canaltech.com.br/internet/o-que-e-firewall/>>. Acesso em: 02 jul. 2020.

FEDERAÇÃO BRASILEIRA DE BANCOS (Febraban). **Lista de Bancos**. Disponível em: <<https://www.febraban.org.br/associados/utilitarios/bancos.asp>>. Acesso em: 1º jul. 2020.

JESUS, Damásio de; MILAGRE, Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

KASPERSKY. **O que é ransomware?** Disponível em: <<https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware>>. Acesso em: 1º jul. 2020.

MERCÊS, Fernando. O que fazer antes que seu celular seja roubado. **Mente Binária**, 14 de maio de 2019. Disponível em: <<https://www.mentebinaria.com.br/artigos/o-que-fazer-antes-que-seu-celular-seja-roubado-r44/>>. Acesso em: 03 jul. 2020.

MINISTÉRIO PÚBLICO DE MINAS GERAIS. **Navegar com Segurança**: por uma internet mais segura, ética e responsável. 4 ed. Belo Horizonte: MPMG, 2019.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. Comitê Gestor da Internet no Brasil. **Guia #Internet com Resposta**: Cuidados e responsabilidades no uso da Internet. 2018. Disponível em: <<https://www.cgi.br/publicacoes/indice/guias/>>. Acesso em: 1º jul. 2020.

OLIVEIRA, Wilson. **Técnicas para hackers e soluções para segurança**. 2. ed. Portugal: Centro Atlântico, 2003.

ROCHA, Marcelo Hugo da. **Manual de Dicas**: Analista e Técnico do INSS. São Paulo: Saraiva, 2015.

SAFERNET. **Sextorsão?** Disponível em: <<https://new.safernet.org.br/content/o-que-%C3%A9-sextors%C3%A3o#>>. Acesso em: 1º jul. 2020.

STIVANI, Mirella. O que é um worm? Entenda o malware que se multiplica sozinho. **TechTudo**, 08 de novembro de 2018. Disponível em: <<https://www.techtudo.com.br/noticias/2018/11/o-que-e-um-worm-entenda-o-malware-que-se-multiplica-sozinho.ghml>>. Acesso em: 02 jul. 2020.

VALENTE, Jonas. Brasil tem 134 milhões de usuários de internet, aponta pesquisa. **Agência Brasil**, Brasília, 26 de maio de 2020. Disponível em: <<https://agenciabrasil.ebc.com.br/geral/noticia/2020-05/brasil-tem-134-milhoes-de-usuarios-de-internet-aponta-pesquisa>>. Acesso em: 30 jun. 2020.

WHATSAPP. **Como utilizar confirmação em duas etapas**. Disponível em: <https://faq.whatsapp.com/general/verification/using-two-step-verification?lang=pt_br>. Acesso em: 04 jul. 2020.

WEBSHARE. **O que é Browser ou Navegador?** Disponível em: <<https://www.webshare.com.br/glossario/o-que-e-browser-ou-navegador/>>. Acesso em: 03 jul. 2020.

MATERIAIS COMPLEMENTARES

BALANÇO GERAL. **Golpista falsifica anúncio e engana vendedor e comprador ao mesmo tempo.** (2019). Disponível em:

<<https://www.youtube.com/watch?v=zNyVie0Ysfl>>. Acesso em: 31 jul. 2020.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança na Internet:**

Fascículo Dispositivos Móveis. Disponível em: <<https://cartilha.cert.br/fasciculos/internet-banking/fasciculo-internet-banking.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Privacidade. Disponível em: <<https://cartilha.cert.br/fasciculos/privacidade/fasciculo-privacidade.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Senhas. Disponível em: <<https://cartilha.cert.br/fasciculos/senhas/fasciculo-senhas.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha Internet segura para seus filhos.** Disponível em: <<https://internetsegura.br/pdf/guia-internet-segura-pais.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Comércio Eletrônico. Disponível em: <<https://cartilha.cert.br/fasciculos/comercio-eletronico/fasciculo-comercio-eletronico.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Códigos Maliciosos. Disponível em: <<https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Backup. Disponível em: <<https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Redes Sociais. Disponível em: <<https://cartilha.cert.br/fasciculos/redes-sociais/fasciculo-redes-sociais.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Redes. Disponível em: <<https://cartilha.cert.br/fasciculos/redes/fasciculo-redes.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Verificação em Duas Etapas. Disponível em: <<https://cartilha.cert.br/fasciculos/verificacao-duas-etapas/fasciculo-verificacao-duas-etapas.pdf>>. Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Computadores. Disponível em: <<https://cartilha.cert.br/fasciculos/computadores/fasciculo-computadores.pdf>>.

Acesso em: 31 jul. 2020.

_____. **Cartilha de Segurança na Internet:** Fascículo Internet Banking – arquivo .PDF. Disponível em: <<https://cartilha.cert.br/fasciculos/internet-banking/fasciculo-internet-banking.pdf>>. Acesso em: 31 jul. 2020.

DOMINGO ESPETACULAR. Golpe do falso leilão cresce durante a pandemia: Veja a Matéria do Domingo Espetacular. (2020). Disponível em: <<https://www.youtube.com/watch?v=VWZvyfXUxNk>>. Acesso em: 31 jul. 2020.

GOOGLE FOR EDUCATION. Proteção contra phishing e golpes. (2017). Disponível em: <<https://www.youtube.com/watch?v=0Sis2KAeKsU&feature=youtu.be>>. Acesso em: 31 jul. 2020.

HENIS, Débora. Sofri um golpe no mercado livre! (2020). Disponível em: <https://www.youtube.com/watch?v=6C3_46wm5uY>. Acesso em: 31 jul. 2020.

HOJE EM DIA. Saiba como se proteger do golpe da clonagem do WhatsApp. (2020). Disponível em: <https://www.youtube.com/watch?v=0mN_WQJ_J4M>. Acesso em: 31 jul. 2020.

MG INTER TV. Policia Civil investiga ocorrências de golpes de boletos falsos em Montes Claros. (2018). Disponível em: <globoplay.globo.com/v/7106735/>. Acesso em: 31 jul. 2020.

REPORTAGEM: Ransomware no Brasil. (2018). Disponível em: <<https://www.youtube.com/watch?v=kzuwmF1W2fE>>. Acesso em: 31 jul. 2020.

SAFERNET BRASIL. O que é sextorsão? (2018). Disponível em: <<https://www.youtube.com/watch?v=hY7MSSwMYxk&feature=youtu.be>>. Acesso em: 31 jul. 2020.

SAFERNET. Exploração sexual infantil afeta todos nós: Vídeo 2. (2014). Disponível em: <<https://www.youtube.com/watch?v=84VGPqx7x2w&feature=youtu.be>>. Acesso em: 31 jul. 2020.

_____. **Fale sobre Sextorsão.** Disponível em: <<http://www.safernet.org.br/sextorsao/dicas-responsaveis.pdf>>. Acesso em: 31 jul. 2020.

SOBREVIVENDO NA TURQUIA. O golpe do amor sofisticado: "Ele me mandava vídeos!" Diz a vítima. (2020). Disponível em: <<https://www.youtube.com/watch?v=lR9-RYudxC0&feature=youtu.be>>. Acesso em: 31 jul. 2020.

TV BRASIL. Receita Federal alerta para o chamado "golpe do amor". (2018). Disponível em: <<https://www.youtube.com/watch?v=jbpHSxFCDuY>>. Acesso em: 31 jul. 2020.