

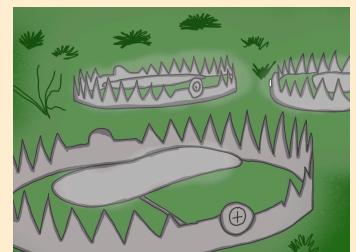
# Como Navegar na Web de Forma Segura



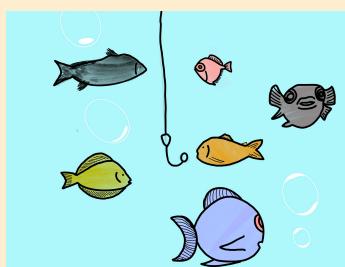
O que são DADOS



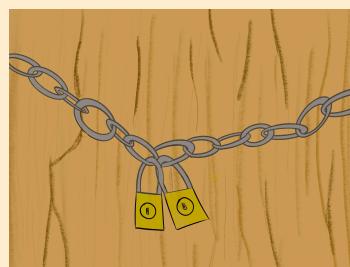
VÍRUS



Armadilhas



PHISHING

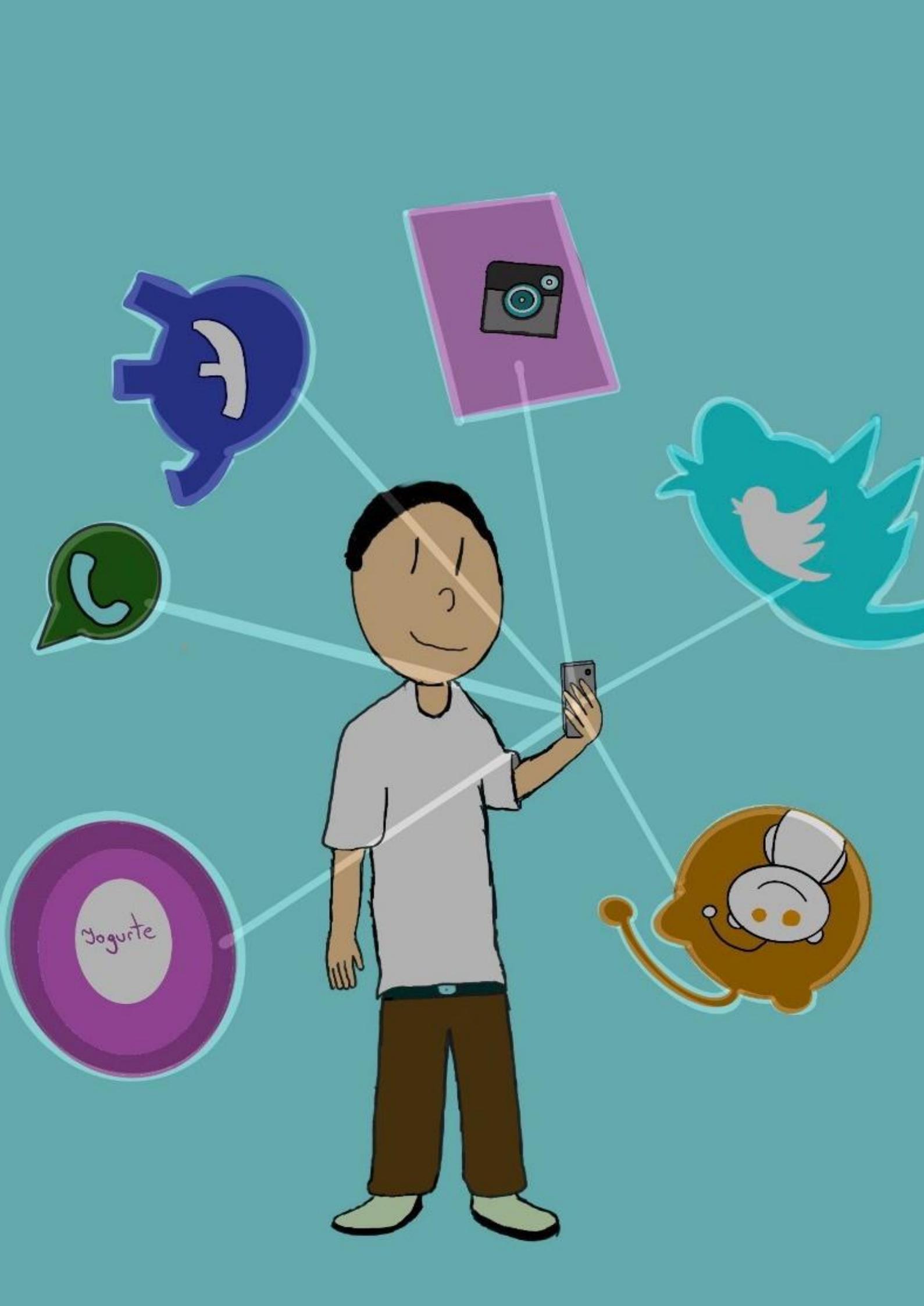


Como se Proteger

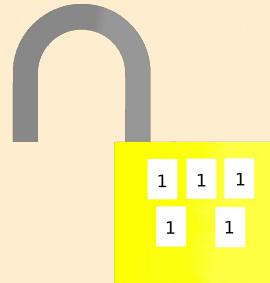


INSTITUTO DE COMPUTAÇÃO

Gustavo Avalos de Almeida  
Henrique de Oliveira Peixoto  
Lucas Eduardo Romero  
Thiago Strussmann Nunes da Cunha  
Victor Hugo Maranholi



Yogurte



## O QUE SÃO DADOS?

Considere um cenário no qual você está fazendo compras em uma loja de sapatos, e o pagamento será feito por cartão de crédito. O funcionário do caixa pede para que você assine a nota de compras e digite a senha do seu cartão. Ao ler a nota, você identifica informações à respeito da loja, do produto e sobre você. Essas informações estão dispostas de modo que facilite a compreensão, por exemplo:

Valor ..... R\$ 59,99

Aqui temos a informação de um produto cujo valor são R\$ 59,99. Isso é um dado. Dados são informações que possuem algum sentido, como “nome: João da Silva”, “cartão: mastercard”, “número do cartão: 0123.4567.8910”, etc. Perceba que todos os dados estão “catalogados” de modo a possuírem algum sentido. Se separarmos “joão da silva” de “nome”, não podemos determinar o que é “joão da silva”, pois pode ser o nome de uma rua, escola, placa, marco ou uma empresa. Portanto, o marcador “nome” é utilizado para completar o sentido da informação “Nome: João da Silva”.

Num sistema digital, esses dados ficam armazenados em um tipo de programa que chamamos de Banco de Dados. Como o nome sugere, banco de dados é um tipo de software (programa) que armazena dados. É neste tipo de programa que ficam armazenadas suas senhas de e-mail, dados de cadastro nas redes sociais, fotos postadas no Facebook e até mesmo seu histórico de navegação no site da Google. Essas informações sobre você (seus dados) ficam armazenados para serem acessados sempre que alguém precise deles. Considere o exemplo:

Log in

Username

Password

Log in

Remember me      [Forgot Password?](#)

[Create an Account](#)

Ao lado há uma típica tela de *login* (autenticação) de usuário. Quando você digita seus dados de acesso, o sistema realiza uma consulta no banco de dados e verifica se as informações que você digitou são as mesmas que estão no banco. Uma mensagem será retornada informando se você realizou o procedimento de autenticação com sucesso ou se alguma das informações digitadas está errada.

Outro exemplo de dados pessoais são as informações de navegação que você guarda no navegador e nos históricos dentro dos sites que você navega. Ao realizar uma consulta no Google sobre “camisa verde”, o serviço de busca irá exibir uma consulta com uma série de links que possuem relação com “camisa verde”. Ao clicar em um link específico da consulta, você é redirecionado para o site que possui uma camisa verde, que custa um preço X e possui X características. Entretanto, você retorna ao Google e procura a mesma camisa em outros sites, até ter completado seu orçamento e decidido onde irá comprar sua camisa verde. Um procedimento simples, com apenas algumas consultas e uma compra realizada com sucesso, certo? Na verdade, não é tão simples.

## SEU HISTÓRICO, MEU LUCRO

Esses dados presentes nos bancos de dados dos sites são inseridos, principalmente, quando você preenche o formulário de cadastro daquele site. Além disso, há muitos dados que são compartilhados entre os sites. Digamos que você possui uma conta no Banco do Brasil. Este compartilhará seus dados com o Banco Central, com os serviços de proteção de crédito (SERASA/SPC), e podem até fornecer seus dados para terceiros. Por isso é importante se manter atento em quais sites você realiza cadastro de conta, pois seus dados estarão armazenados no banco de dados daquele serviço. Não é à toa que muitos sites fornecem conteúdo “gratuito”, pois o interesse deles são as informações sobre você e as redes sociais são um exemplo disso.

Esse tipo de coleta é bem fácil de perceber na prática. Se você usa o YouTube no seu celular, abra o aplicativo e analise suas recomendações. A sua página inicial deve ser bastante precisa em relação ao tipo de conteúdo que você gosta. Se o leitor quiser observar a diferença, basta abrir o navegador, iniciar uma guia anônima e abrir o YouTube (ou abrir as configurações do aplicativo e entrar no modo anônimo). Verá que como o YouTube não identificou o usuário, as recomendações muito provavelmente não estarão adaptadas aos seus gostos.

O motivo é a ausência de informações coletadas sobre você. Portanto, uma dedução simples que poderia ser feita é: o YouTube usa os vídeos que o usuário assistiu para determinar quais outros podem ser interessantes. E isso é vantajoso para a plataforma, visto que, quanto mais conteúdo consumido maior é a quantidade de anúncios exibidos. É uma forma de manter o usuário interessado na plataforma. Netflix também faz uso de ferramenta similar, mas não é com o mesmo objetivo.

De forma simplificada, o seu histórico é bastante útil para as empresas na manutenção e personalização de seus serviços. E mais, ela pode vender essas informações para outras empresas que querem vender algum produto à você.

## O QUE A INTERNET SABE SOBRE NÓS

Agora que o leitor já foi apresentado ao conceito de dados, neste capítulo demonstraremos o que a internet pode saber sobre nós.

Suponha que você deseje pegar um livro emprestado em uma biblioteca, mas não possui cadastro. Ao chegar lá, antes de qualquer coisa, você se direciona à secretaria do local e faz o cadastro em questão. Obviamente, a pessoa que te atender irá pedir alguns “dados” sobre você, tais como nome, data de nascimento, RG/CPF, endereço, telefone e a lista continua... Esses dados que você forneceu à instituição agora permitem que você tenha acesso às estantes e pegue um livro emprestado. Consideremos o Facebook. Você cria sua conta através de um formulário de cadastro, onde você irá inserir algumas informações sobre você. Após realizar a autenticação, você pode adicionar amigos, ver o conteúdo que eles acessam e compartilhar aqueles dos quais você gostar. Enquanto isso, o Facebook terá coletado informação a respeito de quem são seus amigos, qual tipo de pessoa você prefere adicionar e quais as localidades em comum dessas pessoas. Além disso, ele sabe qual conteúdo você prefere acessar e gosta de compartilhar. Com estas informações, a plataforma é capaz de selecionar os melhores anúncios que coincidem com seu histórico de navegação.

Essa é a forma mais simples e direta de coleta de dados. O processo de cadastro nada mais é que preencher um formulário com informações que o sistema pede antes de tirar proveito de um serviço.

Agora serei obrigado a informar-lhe, meu caro leitor, que existem muitas outras informações que você provavelmente entrega de bandeja aos sites que visita. Isso muitas vezes de forma invisível, porém com seu *consentimento*.

Exatamente, toda informação coletada sobre você de forma “secreta” (considerando que estamos falando de uma empresa que segue a legislação) é disponibilizada porque você permitiu.

Aqui entram em cena: *cookies* (serão explicados depois, no momento só estão aqui para dar fome mesmo), acesso à história de navegação, informações que o seu computador entrega e aquelas mensagens irritantes que surgem espontaneamente, e você teve o azar de estar com o mouse ou o dedo no botão “Sim”...

Se você possui alguma noção um pouco mais avançada sobre informática, recomendamos que o leitor visite o *Webkay*. Trata-se de um site que exibe quais dados o seu navegador disponibiliza para toda a internet. Isso mesmo, seu navegador dedura bastante coisa. Mas calma que não há motivo para se preocupar, a princípio. A maior parte das informações são sobre as peças de seu dispositivo e o programa que está sendo usado para navegar. Isso é para permitir que os sites se ajustem ao dispositivo em questão e é por isso que você consegue abrir certas páginas tanto em computadores como em celulares e o conteúdo se ajusta muito bem.

Mas a história não se encerra por aqui. Tem certas informações um pouco diferenciadas que são liberadas por aí. Por ter chegado até aqui, daremos uma prévia do porque você deveria se importar com esses dados.

## TESTE VOCÊ MESMO

Se você está com seu smartphone por perto, faça um teste caseiro. Com o aparelho na Tela Inicial, diga “Ok Google” ou “Hey Google” no Android. Ainda, caso esteja no iOS, diga “Hey Siri”. Apareceu algo? Se seu celular respondeu como esperado, ele deve ter exibido o aplicativo do assistente pessoal correspondente ao seu sistema.

Você deve estar se perguntando qual a relevância desse feito. Usemos a lógica, para que alguém responda a um chamado seu basta que ele esteja **ouvindo**. Sim, seu aparelho está escutando você durante todo o tempo em que está ligado. Mas não se desespere, o áudio gravado pelo telefone só é enviado aos servidores, quando a frase de ativação acima é detectada. Geralmente, trata-se um áudio que se estende



em aproximadamente 5 segundos. É possível escutar esse áudio em dispositivos Android visitando a página de controle de atividade no Google.

Mas vamos expandir um pouco mais o problema, porque de certa forma, ainda possuímos alguma segurança quando os dados estão na mão de corporações. Como estamos falando de segurança digital, imaginemos um vírus de computador. Tal programa possui a capacidade de infectar periféricos do computador, incluindo câmeras, microfones e até texto digitado no teclado. E conhecendo a índole dos cibes criminosos, não é necessário pensar bastante sobre porque essas informações são bastante sensíveis nas mãos erradas.

## VÍRUS

Essa é uma palavra que escutamos com bastante frequência no cotidiano. Seja na área da saúde ou da computação, é consenso universal que são maléficos. Se até mesmo os vírus se odiasssem ninguém se surpreenderia. É algo cruel, que destrói das formas mais astutas possíveis.

Para explicar melhor o que são vírus, faremos uma ponte com a biologia. Acalme seus nervos porque não iremos entrar em detalhes complexos. Sabemos que alguns leitores têm muitas mágoas a tratar com a biologia, assim como outros têm com a matemática e as outras matérias.

Mas chega de enrolação, chegou a hora de saber o que são vírus e como se proteger.

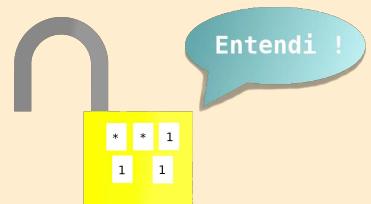
## O QUE SÃO VÍRUS?

No mundo real, vírus são criaturas “programadas” para o caos. Costumam ser sorrateiros, mas há exceções. Existem doenças que levam muitos meses para serem detectadas, enquanto outras te derrubam em alguns dias. Seu objetivo, de forma simples, é se reproduzir infectando células de um organismo, utilizando os recursos do hospedeiro para atingir tal objetivo, geralmente o matando no fim.

Apesar de ninguém morrer por causa de um vírus proveniente daquele jogo pirata que você baixou num site meio obscuro, no computador funciona quase da mesma forma. O vírus se esconde em processos obscuros, infiltrado como um programa qualquer, observando seus passos, coletando informações e se multiplicando. Quando chega o momento de atacarem, pode ocorrer de forma sutil,

como uma leve gripe incômoda, deixando seu computador lento, ou pode ser um pouco mais brutal, como acontece com o vírus da raiva, que quando contraído e não tratado possui taxa de mortalidade de 100%. No computador, isso seria similar à um programa que corrompe as partes vitais de seu funcionamento, como a parte responsável por fazê-lo iniciar.

Deu para perceber a semelhança, certo? Então, só para formalizar o conteúdo, vírus são programas de computador que possuem um objetivo certamente maléfico ao usuário. Realizam roubo de dados, espionagem (via câmera e microfone), além de corromper arquivos ou o próprio sistema operacional. Se multiplicam e infectam outros computadores, geralmente transferidos pela internet, discos (CDs e DVDs gravados de forma ilegal, por exemplo), pendrives e mídias removíveis em geral. Muitas vezes o estrago causado por esses programas dá tanta “dor de cabeça” que várias pessoas optam por zerar o computador.



## O QUE VOCÊ DESEJA FORNECER?

Uma adição um tanto recente aos dispositivos móveis é o sistema de controle de permissão. Agora os usuários podem determinar que funções do aparelho um determinado aplicativo pode acessar. E, adivinhe... Essa é outra forma de coletar dados.

Quando um aplicativo de mapas pede permissão para acessar sua localização, ele pode fazer o que quiser com essa informação, inclusive traçar um perfil personalizado de você, contendo os lugares que você mais visita, o tempo no trânsito, locais de trabalho ou moradia etc.

As permissões são várias, mas as mais sensíveis são: câmera, gravação de voz, localização, contatos, fazer chamadas e/ou mandar mensagens e até mesmo visualizar o conteúdo da tela, além de bloquear e limpar o dispositivo.

Não é necessário ressaltar que tais permissões são perigosas quando usadas por programas mal-intencionados. Como usuário, você deve cuidar muito de quais permissões são concedidas aos seus aplicativos.

## ARMADILHAS

Agora que já possui uma maior compreensão, você entenderá o porquê você deve se preocupar com esses dados. A seguir, serão explicadas as formas mais comuns de se obter informações sensíveis sobre você utilizada por usuários mal-intencionados.

### NÚMERO DE CELULAR CLONADO

Quando você utiliza um serviço digital que demanda autenticação, é comum haverem solicitações de códigos de segurança que são enviados por SMS ao seu celular. Esses códigos possuem a importância de complementar a segurança da sua conta, como um “extra” para a sua senha. Entretanto, um hacker mal intencionado possui as informações corretas sobre você, ele pode entrar em contato com a sua operadora de telefone, utilizar todos os dados que possui para se passar por você, solicitar alteração de número de telefone para outro chip, que será utilizado em outro dispositivo, e assim ele terá acesso a esses códigos de autenticação que são encaminhados por SMS para poder roubar seus dados de bancos, aplicativos, redes sociais, etc.

### APLICATIVOS FALSOS

Aplicativos são programas que baixamos em nossos celulares para executarmos alguma funcionalidade que não havia nele. Por exemplo, NetFlix. O aplicativo da empresa permite acessar todo o conteúdo disponível em seu catálogo através de um smartphone, por exemplo. Entretanto, há aplicativos que são disponibilizados com más intenções, e têm o objetivo de roubar informações do seu aparelho, ou exibir informações e anúncios indesejados.

Neste ano, pesquisadores de segurança da *Eset* e *Trend* (empresas de antivírus) registraram mais de noventa aplicativos falsos no *Google Play Store*. Juntos, esses programas falsos somam mais de dezessete milhões de download falsos. A Google possui um sistema automatizado de proteção contra aplicativos falsos, e direciona esforços humanos para auxiliar na identificação de falsos aplicativos, mas a

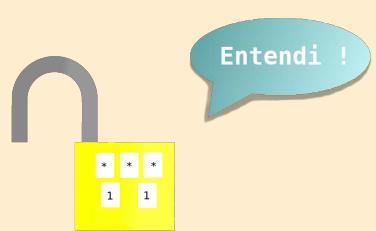
maior proteção é a atenção. Sempre desconfie de aplicativos com aparência estranha, leia as avaliações nas suas descrições, e pesquise sobre antes de fazer download.

## NOTÍCIAS FALSAS

As redes sociais surgiram com uma proposta de conectar pessoas distantes. Com o decorrer dos anos, as plataformas se tornaram um meio de divulgação, inclusive de notícias. Hoje, o Facebook é a maior plataforma de divulgação de informações do mundo, tornando acessível diferentes jornais e sites de notícias que antes eram desconhecidos.

Entretanto, pessoas maliciosas usam estas plataformas para propagar links com títulos chamativos, atraindo usuários desatentos que entrem na página direcionada pelo *link*. Essa técnica é chamada de *phishing*, e pode ser usada para diferentes demandas de fraude. Ao clicar em um link de uma notícia falsa, você pode ser direcionado para um site onde há diversos links de pesquisas falsas que irão roubar seus dados inseridos em seus campos de inserção de informações. Além disso, existe a possibilidade de você ser direcionado para uma página que é idêntica a um site onde você tem conta. Entretanto, este site é falso e irá capturar suas informações inseridas, principalmente as de autenticação, para serem utilizadas contra você, posteriormente.

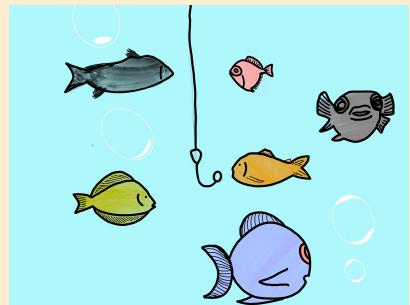
Por isso, é sempre importante manter atenção aos endereços de sites de uma página que você está acessando.



## PHISHING

O *phishing* é uma forma de fraude por meio do roubo de dados pessoais, que são posteriormente utilizados para cometer outras fraudes. O *phishing* pode aparecer de diversas formas, mas tem como elemento comum se passar por alguém ou por uma empresa conhecida, e usar da curiosidade ou preocupação da pessoa para que o próprio usuário passe as informações pessoais.

Este tipo de ataque pode ocorrer por diversos meios, sejam eles telefone, correios ou e-mail. Exemplos comuns são de se passar por empresas fazendo promoções, ou por bancos pedindo atualização de dados cadastrais. As formas mais comuns de phishing vem por meio dos seguintes meios:



## E-MAILS FRAUDULENTOS

Os serviços de fornecimento de e-mail (hotmail, gmail, yahoo, etc...) possuem uma proteção nativa dentro de suas plataformas, o serviço de spam. Esta caixa indicará possíveis e-mails que carregam algum *malware* (vírus) que podem te prejudicar. Entretanto as vezes falha e, portanto, é importante manter o máximo de atenção ao abrir e-mails, pois além de *links* falsos, que servem apenas para roubar seus dados, algumas mensagens recebidas carregam algum tipo de vírus que pode comprometer, além de seus dados, todo o seu equipamento de acesso.

O tipo de golpe mais frequente, o golpista redireciona a vítima a um site falso onde ele pode obter informações da vítima sem que esta perceba. É comum o fraudador enviar um email se passando por um banco, com alguma mensagem de caráter urgente, como por exemplo dizendo que a conta da vítima está bloqueada e precisa atualizar informações, ou alguma loja oferecendo uma promoção muito atrativa. Nestes casos eles fornecem links para a vítima resolver o problema ou ver a oferta, mas acabam sendo redirecionadas para sites falsos, com design e nomes muitos similares aos legítimos, mas onde todos os dados digitados pelo usuário são salvos pelos golpistas.

Figura 3 - Exemplo phishing por site falso.

The screenshot shows a Microsoft Internet Explorer window with the title 'Banco ... - Feito Para Você - MS Internet Explorer'. The address bar displays the URL 'http://www.its.ilstu.edu/ftug/indexIE.html'. The main content area is a Bankline login page. At the top, there's a navigation bar with tabs like 'Bankline', 'AGÊNCIA', 'CONTA', 'OK', and 'Poder Público'. Below the navigation, there's a form for logging in with fields for 'Agência', 'Conta', 'Senha Eletrônica', 'Senha do Cartão', '5 Dígitos do Cartão', and 'Data de Nascimento'. A large red arrow points from the left towards the address bar. Another red arrow points from the right towards the card number input field, which contains a sample card number (0500 02070-2 58L XXXXXX T-X). On the left side of the form, there's a note: 'Digite os números que constam no seu cartão conforme exemplo ao lado.' Below the form, there are several promotional banners: 'Dicas de Segurança' (with a note about checking the bankline before entering the password), 'Leilão de Imóveis' (mentioning 'As melhores oportunidades de imóveis com as condições ideais para você.'), 'Banco' (mentioning 'A marca ... foi eleita mais uma vez a mais valiosa do Brasil.'), 'SUPERNOVAS' (mentioning 'As melhores oportunidades de imóveis com as condições ideais para você.'), 'Inscrições prorrogadas' (mentioning 'Faça já a sua inscrição no Prêmio Escrevendo o Futuro até o dia 14/06.'), and 'É dia de ganhar com .card.' (mentioning 'Participe desta promoção exclusiva: são 92 prêmios de R\$3.000,00, um para cada dia da promoção!'). At the bottom of the page, there's a footer with links like 'Relações com Investidores', 'Imprensa', 'Notícias e Cotações', 'Cultural', 'Social', 'Oportunidades de Carreira', 'Segurança e Privacidade', and 'Fale Conosco'. The status bar at the bottom shows the URL 'http://www.itau.com.br/poderpublico/index0.htm' and the word 'Internet'.

Fonte: livro Manual das Fraudes - 2.a ed.

Perceba na figura 3 como o layout é similar ao do banco verdadeiro, porém o link é diferente. Neste caso, uma vítima desatenta poderia fornecer seus dados bancários ao golpista

Figura 2 - promoção falsa recebida no email



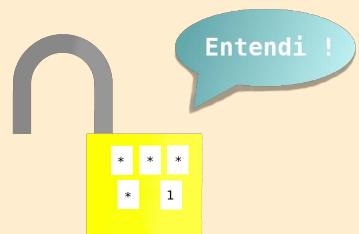
Fonte: <https://www.lumiun.com/blog/phishing/>

Repare na imagem 2 como no email eles fornecem um botão para serem redirecionados para a “promoção”, e na parte de baixo como o link não tem relação com a empresa original.

## SMISHING

Similar ao *phishing*, porém são recebidos por mensagens de SMS contendo um link para um site falso, que pede ao usuário que o acesse. Outras modalidades pedem que o usuário baixe um aplicativo, que funcionaria como um espião no celular da vítima.

Figura 3 - Exemplo Smishing.



## COMO SE PROTEGER

Então você entendeu os perigos que rodeiam a internet e quer se proteger? Nesta seção abordaremos as atitudes, na prática, que você pode tomar para navegar blindado na Web.

### SENHAS

Uma pesquisa realizada por especialistas em segurança da *LogMeIn* com mais de 2000 usuários de países como Estados Unidos, Austrália, França, Alemanha e Reino Unido revelou que 91% dos entrevistados sabem que é perigoso reutilizar a senha e ainda assim, 51% o fazem.

É comum na internet os usuários utilizarem as mesmas senhas para vários sites diferentes. Vamos admitir, é mais conveniente utilizar sobrenome ou data de aniversário porque é mais fácil de memorizar. Quem esqueceria sua própria data de nascimento? O problema é que todo mundo sabe disso, para o bem ou mal... Sabendo disso, como podemos definir senhas boas e fáceis de lembrar? Com a criatividade em dia, o céu é o limite:

- 1 - Crie uma frase sonora e boa de lembrar  
Cascadura de roer
- 2 - Substitua algumas letras por caracteres especiais

C4\$cadur4 de ro3r

3 - Misture letras maiúscula e minúsculas

C4\$CadUr4 de RO3r

4 - Tempere a senha

C4\$AdUr4@de@RO3r

Agora você tem uma senha, e para não jogar fora todo nosso trabalho de criar a senha, existem regras que devem ser seguidas

1- Nunca empreste sua senha: Um antigo ditado diz que “O segredo melhor guardado é o que a ninguém é revelado”, portanto não importa a força da sua senha, se você conta a alguém ela se torna fraca imediatamente.

2 - Não anote sua senha em lugares de fácil acesso, como em arquivos de texto ou na área de trabalho do computador: Seus backups devem estar bem protegidos, guardados longe do acesso de visitantes no computador. Guarde-os em um HD externo no seu armário, por exemplo.

3 - Não use a mesma senhas em diversos serviços: Como mencionado anteriormente, repetir a senha é o maior pecado que um usuário pode cometer. Crie diversas senhas diferentes.

E como usar diversas senhas e se lembrar de todas ? Nesse momento, você precisará de um gerenciador de senhas.

## GERENCIADORES DE SENHAS

Esta tecnologia permite guardar senhas com segurança e de forma muito prática pois os melhores gerenciadores - com poucos cliques - geram senhas aleatórias e salvam seu login para uma futura autenticação automática. Bem prático, né? Muitas pessoas usam sem perceber o gerenciador de senhas da Google, do Firefox ou qualquer outro navegador, mas é importante entender como funciona e os riscos. Para usar um gerenciador, você precisará usar uma chave-mestra: Uma senha que te dará acesso à todos seus outros dados sensíveis. Ou seja, essa tem que ser “A senha”, pois é o principal ponto de ataque dos invasores.

Escolha o Gerenciador de senhas que mais lhe agradar, como do seu navegador, e tome cuidado ao deixar o login automático ativado. Apenas quem deixou

uma rede social autenticada, voltou e tinha sido sacaneado sentiu uma palinha do problema, então evite.

## SEJA CÉTICO

Desconfie de promoções muito atrativas, ou de situações de urgência, principalmente provenientes de bancos e empresas. Criminosos tentam forçar as vítimas a pensarem de forma impulsiva para que não notem o golpe.

Nunca confie em links. Seja por email, SMS ou whatsapp, não use links que lhe forem enviados. Eles podem ser redirecionados para páginas com outros nomes, e com aparência e nomes similares para se disfarçar.

Não forneça senhas ou dados quando lhe forem pedidos por e-mails ou ligações que você tenha recebido. Se preciso, encerre o atendimento e busque você iniciar o contato com o prestador de serviço para ter certeza que está falando com um funcionário legítimo.

Se ficou na dúvida se existe algum problema com o seu banco ou uma oferta, use o seu navegador para procurar o site legítimo e acessá-lo de forma segura ou para procurar o telefone oficial.

## COMPUTADORES PÚBLICOS

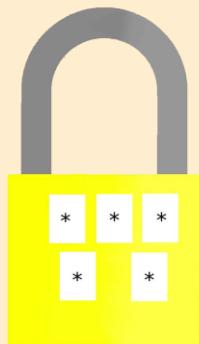
Ao entrar em sua conta bancária, você confia a sua senha ao banco. Você confiaría sua senha a um desconhecido? Os bancos possuem um dos sistemas mais seguros para o qual você pode depositar a sua senha, isso porque o “sistema imunológico” deles é quase perfeito. Ainda assim é difícil efetuar operações apenas no caixa eletrônico.

Perdendo apenas para os computadores públicos, os pessoais são os mais suscetíveis à ameaças. Isso porque estes dispositivos não são adequadamente “blindados”, por mais que se esforce para se proteger, sempre haverá uma brecha que pode ser explorada.

Os computadores públicos, por serem utilizados por todo o mundo, é vulnerável às atividades alheias. Alguém pode, maliciosamente, instalar uma armadilha no aparelho apenas para capturar seu alvo. E esse sujeito pode ser você. A lógica por trás é bastante simples, como existem inúmeras pessoas utilizando o computador, a

chance de se obter um “pescado” com uma rede é bem maior se comparado a utilizar um anzol.

Deve-se, portanto, tomar cuidado ao nadar em um rio sem alcançar o fundo, por mais que saiba nadar e que esteja equipado, nunca se sabe pra onde a correnteza o levará e se haverá obstáculos no caminho.



**PARABÉNS, AGORA VOCÊ SABE COMO SE PROTEGER NA INTERNET**



## REFERÊNCIAS POR SESSÃO

### 1- O que são Dados

**GLOBALENSIGN.** What Data Is Collected About You Online and How to Stop It. [S. I.], 15 jun. 2018. Disponível em: <https://www.globalsign.com/en/blog/what-data-is-collected-about-you-online/>. Acesso em: 17 dez. 2019.

**LINUS**, Robin. What Every Browser Knows About You. [S. I.], [S.D.]. Disponível em: <https://webkay.robinlinus.com/>. Acesso em: 17 dez. 2019.

### 2 - Phishing

**LUMIUN**, Phishing: como se proteger e não cair no golpe. Disponível em <https://www.lumiun.com/blog/phishing/>.

**INFOWESTER**, O que é phishing? E como evitar golpes do tipo?. Disponível em <https://www.infowester.com/phishing.php>.

**FRAUDES.ORG**, Pishing, Falsos sites de bancos. Disponível em <http://www.fraudes.org/showpage3.asp?pg=298>

**PARODI, L.** Manual das Fraudes : 2 e.d: Editora Brasport.

### 3 - Vírus

"**VÍRUS**" em Só Biologia. Virtuous Tecnologia da Informação, 2008-2020. Consultado em 03/02/2020 às 20:41. Disponível em <https://www.sobiologia.com.br/conteudos/Seresvivos/Ciencias/biovirus.php>.

**EQUIPE MEGACURIOSO**. Confira 6 dos vírus mais letais do planeta. [S. I.], 22 mar. 2018.

Disponível em: <https://www.megacurioso.com.br/virus-bacterias-e-protozoarios/101672-confira-6-dos-virus-mais-letais-do-planeta.htm>. Acesso em: 7 fev. 2020.

**KASPERSKY**. What Malware Needs to Thrive. [S. I.], [S.D.]. Disponível em: <https://www.kaspersky.com/resource-center/threats/hacking-system-vulnerabilities>. Acesso em: 7 fev. 2020.

**KASPERSKY**. How do computer viruses work?. [S. I.], [S.D.]. Disponível em: <https://www.kaspersky.com/resource-center/threats/how-to-get-rid-of-a-computer-virus>. Acesso em: 8 fev. 2020.

**WORLD HEALTH ORGANIZATION**. Q&A on vaccines. [S. I.], 26 ago. 2019. Disponível em: <https://www.who.int/vaccines/questions-and-answers>. Acesso em: 8 fev. 2020.

**HOFFMAN**, Chris. How Antivirus Software Works. [S. I.], 26 set. 2016. Disponível em: <https://www.hoffman.com/antivirus-software-works>

## **Créditos**

**Gustavo Avalos de Almeida** - Produção de imagens e redator

**Henrique de Oliveira Peixoto** - Redator

**Lucas Eduardo Romero** - Desenvolvedor e designer

**Thiago Strussman Nunes da Cunha** - Redator

**Victor Hugo Maranholi** - Redator e Designer