SEGURANÇA
NA INTERNET
A PRAÇA PÚBLICA VIRTUAL

iStart Ética Digital
Peck Advogados
CREDILINK® INFORMAÇÕES DE CRÉDITO

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Segurança na Internet: [livro eletrônico] : a praça pública virtual / Larissa C. Lotufo da Costa ... [et al.] ; coordenação Patrícia Peck Garrido Pinheiro ; ilustração Junior Meneguette. -- 1. ed. -- São Paulo : iStart Ética Digital, 2021.
PDF

Outros autores : Diago Savio M. de M. Sucar, Felipe Mury Botelho, Anna C. Leonetti do S. Janni.
ISBN 978-65-995083-0-1

1. Crimes digitais 2. Direito digital 3. Proteção de dados - Direito - Brasil 4. Proteção de dados - Leis e legislação 5. Proteção de dados pessoais I. Pinheiro, Patrícia Peck Garrido. II. Meneguette Junior. III. Sucar, Diago Savio M. de M. IV. Botelho, Felipe Mury. V. Janni, Anna C. Leonetti do S.

21-66914 CDU-342.721(81)

Índices para catálogo sistemático:

1. Brasil : Proteção de dados pessoais : Direito 342.721(81)

Aline Graziele Benitez - Bibliotecária - CRB-1/3129

SUMÁRIO

APRESENTAÇÃO

Parando para refletir, o mundo on-line é como uma grande praça pública, com a diferença de que nesta praça é possível encontrar uma dimensão infinita de possibilidades, sem limites geográficos e barreiras físicas. Completamente diferente da forma como se desenvolveram e se organizaram as nações e seus governos, até a popularização da internet.

O fato é que as tecnologias nascem e evoluem a cada dia, em um ritmo em que pouquíssimas legislações do mundo conseguem acompanhar. Em alguns territórios, o cibercrime já vem sendo mapeado, legislado e julgado há tempos. Em outros, esse ordenamento legal ainda está em processo de elaboração e implantação.

A verdade é que tudo está em constante transformação e mudança, principalmente na Sociedade Digital.

Será que sabemos circular protegidos nas “ruas digitais” do planeta?

Tendo em vista este cenário, a **Credilink**, o **Peck Advogados** e o **Instituto iStart** firmaram uma parceria para orientar quem usa a internet - seja de forma pessoal ou profissional - sobre as melhores práticas de segurança de dados.

Boa leitura!

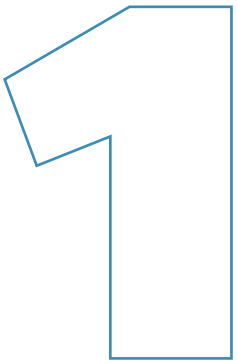
“A desconfiança é a mãe da segurança.”

- Madeleine de Scudéry

01

SOCIEDADE

Mantenha sua segurança onde estiver na “grande praça pública digital”



USE UMA SENHA FORTE E A ALTERE REGULARMENTE

“Senhas fortes”, é assim que são conhecidas as senhas que utilizam diferentes caracteres com o objetivo de dificultar o trabalho de hackers e fraudadores. Criar uma senha forte é muito importante, tendo em vista que, além de conhecer as senhas mais comuns, os hackers utilizam também softwares para descobrir o código de acesso dos usuários. Portanto, todo cuidado é pouco!

NA PRÁTICA

Use números, caracteres especiais e letras sem sequência ou significado. Evite utilizar a própria data de nascimento e números sequenciais. Quanto mais aleatório, melhor!

Exemplo de senha fraca: `Jose12!`

Exemplo de senha forte: `I@y5u0x$`

2 EVITE SALVAR SENHAS AUTOMATICAMENTE

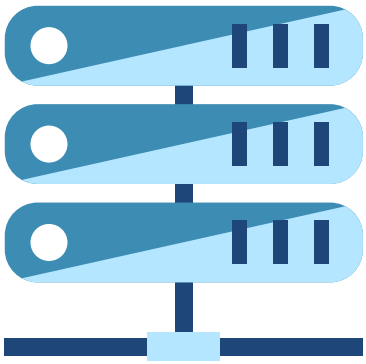
Alguns softwares e navegadores permitem que você salve suas senhas. Verifique o nível de proteção deles! Cuidado para não salvar suas senhas e informações de cartão ou acesso em computadores desconhecidos.

3 ATENÇÃO AO SE CONECTAR ÀS REDES PÚBLICAS DE WI-FI

Antes de se conectar a uma rede pública, certifique-se de que a rede é confiável e, no mínimo, protegida por senha.

LEMBRE-SE

Através de uma rede pública (aberta) é possível acessar dados e pastas do seu dispositivo enquanto ele estiver conectado. O mesmo acontece nas redes corporativas de trabalho.



USE VPN PARA PROTEGER SEUS DADOS PESSOAIS AO NAVEGAR

Em situações normais, toda vez que você se conecta à internet, você é identificado pelo seu número de IP e boa parte de seus dados trafegam abertamente. Em uma VPN (*Virtual Private Network* - Rede Privada Virtual), o usuário pode se proteger de invasões, evitando de ser facilmente identificado.

EM TERMOS GERAIS

A VPN funciona como uma "sub-rede" ou rede privada que oferece ferramentas adicionais de criptografia e navegação sigilosa. Dentro da VPN apenas dois ou poucos computadores conseguem acessar as informações disponíveis, tendo em vista que é um espaço privado e não público.

5

EVITE DIVULGAR INFORMAÇÕES PESSOAIS

Essa é uma dica de segurança geral, mas é válida, especialmente, para sites ou programas não confiáveis. Portanto, não divulgue seus dados em qualquer lugar. É comum fraudadores aplicarem golpes telefônicos ou por mensagens “se passando” por funcionários de call centers de empresas.

Este tipo de golpe é aplicado com a intenção de recolher dados pessoais das vítimas e depois usá-los de forma maliciosa, seja vendendo as informações ou cometendo outros crimes.

6 PROTEJA SUA PRIVACIDADE NAS REDES SOCIAIS

Através das configurações dos sites e apps é possível definir quem poderá ver seus conteúdos compartilhados em tais ambientes. Quem publica conteúdos pode escolher se só os seus "seguidores" poderão ver as postagens ou se elas estarão em modo público, ou seja, disponíveis para qualquer pessoa que navega na internet acessar.

Utilizar tais configurações a seu favor pode ser uma ótima tática de segurança digital. Destaca-se ainda que algumas ferramentas também permitem segmentar o conteúdo para um grupo ou diferentes grupos, garantindo que os usuários realizem uma gestão consciente e flexível de sua privacidade virtual.

NA PRÁTICA

Se for "fechar" o seu perfil, vale revisitar quem são seus atuais seguidores e até removê-los da sua lista para que não acessem mais suas informações. Lembre-se sempre de ter atenção aos dados e informações que você compartilha.

7 NÃO CLIQUE EM LINKS NÃO CONFIÁVEIS OU DESCONHECIDOS

Seja em e-mails, mensagens de SMS, WhatsApp, entre outros, não clique em links aleatórios e/ou desconhecidos e que vão te levar para ambientes estranhos. E, principalmente: não faça downloads de arquivos ou aplicativos de fontes não confiáveis ou desconhecidas. Você poderá abrir uma brecha em sua segurança virtual e, sem querer, instalar softwares maliciosos que podem causar danos irreparáveis em seu aparelho ou mesmo em sua reputação e vida pessoal e/ou profissional.

NA PRÁTICA

Se receber SMS de autenticação de serviços que você não solicitou, não clique na mensagem ou a repasse para terceiros. Exclua a mensagem imediatamente e bloqueie o contato que lhe enviou a mensagem desconhecida.

EXEMPLO DE GOLPE

O famoso golpe do WhatsApp é realizado com base na exploração de vulnerabilidades dos usuários: a curiosidade e falta de cuidado. Neste golpe, terceiros se apropriam das contas dos usuários do WhatsApp e 'se passam' pela vítima, enviando mensagens aos seus contatos pedindo a realização de transferências bancárias em nome do usuário.

8

NUNCA DEIXE DISPOSITIVOS DESBLOQUEADOS

Principalmente em locais públicos, ao se distanciar dos seus dispositivos, faça o respectivo bloqueio deles. Esta simples ação evita que outras pessoas acessem o seu aparelho e peguem informações sensíveis, privadas ou profissionais existentes ali ou até mesmo se passem por você, prejudicando sua imagem ou aplicando golpes em seu nome.

9

CONHEÇA SEUS DIREITOS REFERENTES A SEUS DADOS PESSOAIS

A Lei Geral de Proteção de Dados trouxe uma série de premissas para proteger as informações pessoais, colocando limites e procedimentos para que as empresas e instituições tratem os dados de forma coerente ao prestar um serviço.

- **O Instituto iStart vem constantemente empenhando esforços para que as pessoas conheçam a lei e seus direitos.**
- **O Peck Advogados também disponibiliza conteúdos especializados sobre o assunto.**
- **A Credilink, além de incentivar iniciativas de conscientização, disponibiliza o texto da LGPD na íntegra em seu site.**

02

FAMÍLIA

Com o crescimento do trabalho remoto (home office) e das aulas a distância (EAD), a segurança de internet em casa se tornou **indispensável!**

1

PROTEJA SEU WI-FI

Faça a alteração constante de sua senha do Wi-Fi e configure seus sistemas de proteção de rede de acordo com as indicações do fornecedor.

NA PRÁTICA

Desabilite a função WPS (Wi-Fi Protected Setup) que vem habilitada de fábrica e que pode permitir que outros dispositivos acessem as configurações dos computadores da sua rede.

2

****

ARMAZENE SENHAS EM LUGARES SEGUROS

Anotar senhas em lugares óbvios e de fácil acesso pode ser mais inseguro do que você imagina. Por isso, utilize gerenciadores de senhas confiáveis para armazenar suas chaves de acesso.

3

UTILIZE MAIS DE UM FATOR DE AUTENTICAÇÃO

Sempre que puder e, principalmente, para contas mais vulneráveis a ataques de cibercriminosos como aplicativos de banco, adote a autenticação por dois ou múltiplos fatores. Na autenticação por dois ou mais fatores, além da senha comum, é exigido do usuário a utilização de um token digital, código enviado por e-mail, SMS, entre outros. Isso traz mais uma camada de segurança ao processo de autenticação.

4

OBSERVE E ENSINE AS CRIANÇAS

A internet possui uma série de benefícios se utilizada para fins positivos, mas também está cheia de pessoas má intencionadas e perigos ocultos. Por isso, ensine boas práticas de uso e segurança às crianças desde cedo, assim como é feito na vida analógica em praça pública. O famoso ensinamento “não fale com estranhos” também é válido no mundo virtual.

NA PRÁTICA

Supervisione o uso de internet dos pequenos, indicando as áreas que eles podem utilizar de forma positiva e incentive a educação digital, ensinando boas práticas de produção de conteúdo e exposição de dados. A privacidade é muito importante para os adolescentes, mas isso não impede que seus pais e tutores sejam cuidadosos e sempre atentos ao comportamento virtual de seus jovens.

ESCOLAS MAIS SEGURAS

A legislação também aborda cuidados específicos para a manipulação de dados de menores de idade. O Instituto iStart criou uma cartilha específica com dicas para escolas realizarem o tratamento desses dados e incentivarem o uso da internet de forma segura. Confira gratuitamente clicando abaixo:

DICAS PARA ESCOLAS

SELO CIDADANIA DIGITAL

É do Instituto iStart também a Campanha Cidadania Digital, uma iniciativa que te ajuda a entender a importância dos cuidados que devem ser adotados na internet. Com caráter educativo, ela identifica padrões, culturas e empresas que se preocupam com a proteção de sua privacidade e de sua família. Ao se tornar um apoiador e enviar o seu avatar, você receberá um PIN para que possa usar em seu e -mail e redes sociais. Para conhecer e participar clique abaixo:

CAMPANHA CIDADANIA DIGITAL

5 CUIDADO COM SITES FALSOS DE COMPRAS

Em alguns casos, cibercriminosos criam páginas idênticas ou parecidas com as páginas reais de empresas que possuem credibilidade no mercado. Preste bem atenção e desconfie se algo fugir do comum.
Se o site está estranho, não digite nada sobre você neste ambiente, pois ao digitar suas informações, malfeitores podem se aproveitar dos dados e usar isso para te prejudicar.

NA PRÁTICA

Observe se o site é legítimo checando a URL na barra de endereço, se a página tem certificação digital e, se for uma empresa desconhecida, verifique qual a reputação da empresa em sites como o "Reclame Aqui".

6 SÓ COMPARTILHE INFORMAÇÕES PESSOAIS QUANDO FOR NECESSÁRIO

Acredite, esta simples conduta analítica evita fraudes e golpes! Seja por telefone, WhatsApp ou até por e-mail. Quadrilhas ‘se passam’ por empresas e ofertam produtos, serviços, vagas de emprego e até fazem cobranças de pagamento para tirar seus dados e aplicar uma fraude contra você.

7 ATIVE AS NOTIFICAÇÕES DE ALERTA DE SUA CONTA BANCÁRIA

Habilite alertas via notificação do seu celular ou envio de mensagens para quando houver o uso de cartão de crédito, débito ou mesmo saque. Se perceber algo de errado, aja com rapidez e entre em contato com a instituição. Essa agilidade na percepção e ação é sempre importante.

8

ATENÇÃO AOS CONTEÚDOS ÍNTIMOS

Ao registrar, armazenar e compartilhar fotos e vídeos íntimos, tenha bastante atenção e cuidado. O vazamento desses conteúdos pode acontecer de forma intencional ou não, mas os prejuízos são imensuráveis.

03

EMPRESA

EM
PRE
SA

Na empresa é muito importante se manter seguro para proteger dados profissionais e pessoais, tanto dos funcionários quantos dos clientes, ainda mais com a LGPD

1

NÃO FIQUE PARA TRÁS: SEJA UM USUÁRIO ATUALIZADO!

Baixe as atualizações dos softwares e aplicativos sempre que estiverem disponíveis, não deixe para mais tarde! Lembre-se: essas atualizações não só corrigem falhas, mas também reforçam a segurança dos ambientes digitais. Então quanto mais atualizado, mais seguro é o seu ambiente virtual.

2

FAÇA O BACKUP REGULARMENTE

Tenha como rotina realizar a cópia de segurança dos seus arquivos, evitando que todos os dados se percam em situação de incidente de segurança. Por exemplo, caso o computador ou a rede de armazenamento possam ter problemas e os arquivos se tornem indisponíveis. Existem softwares que realizam o backup automático, a partir da periodicidade que você escolher.

3

PROTEJA INFORMAÇÕES E AMBIENTES COM CRIPTOGRAFIA E FIREWALL

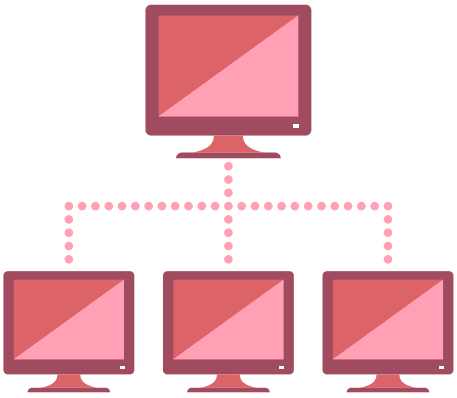
A criptografia é uma forma de transformar a troca de informações de uma rede em códigos que dificultam ainda mais a interpretação dos dados. Por sua vez, o Firewall tem por objetivo aplicar uma política de segurança a um determinado ponto da rede para proteger informações e ambientes, evitando que informações indesejadas entrem ou saiam sem permissão.

NA PRÁTICA

A criptografia pode ser ativada por configurações do sistema do computador ou dispositivo em uso. Já o firewall pode ser adotado a partir da instalação de programas (softwares) ou de equipamentos físicos (hardwares).

4 ADOTE NÍVEIS DE ACESSO À INFORMAÇÃO

Implemente medidas de controle ao acesso de informações e dados da sua empresa, classificando o conteúdo e criando diferentes tipos de usuário para acessá-los.



NA PRÁTICA

Existem informações que só são importantes para a gestão, da mesma forma que existem informações que só interessam e devem ser acessadas pelo financeiro, como faturas e detalhes de pagamento, a equipe de gestão deve cuidar para haver um tratamento adequado dos dados pessoais dos clientes e dos funcionários.

Por isso adotar controles diferenciados por usuários e classificação de dados é de extrema importância, além de ser uma medida básica de proteção digital do ambiente corporativo.

5 PROTEJA SUA IDENTIDADE DIGITAL CORPORATIVA

Adote senhas fortes e diferentes nos ambientes digitais e sistemas da empresa. Não compartilhe a sua senha! Lembre-se: falsa identidade é crime! Além disso, use somente gerenciadores de senhas confiáveis e crie uma chave mestre bastante segura utilizando caracteres especiais, letras maiúsculas e minúsculas, associadas com números.

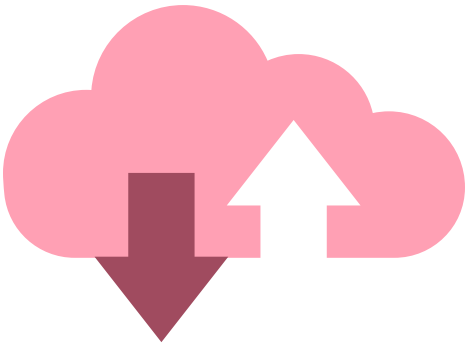
6 CERTIFIQUE-SE DE QUEM ESTÁ DO OUTRO LADO

No contexto do trabalho remoto, é ainda mais importante garantir a identificação segura de todos. Por isso, adote a autenticação por dois ou múltiplos fatores (2FA ou MFA) ou sistema de usuário único (single-sign-on) como padrão em sua empresa.

7

UTILIZE BOAS PRÁTICAS DE COMPLIANCE E SEGURANÇA DA INFORMAÇÃO

Neste sentido, o termo de conscientização de uso da internet entre os colaboradores é fundamental para deixar as regras consolidadas e resguardar a própria empresa sobre possível desvio de conduta.



8 ATENÇÃO AO USO, ARMAZENAMENTO E TROCA DE DADOS DE CLIENTES

Para fazer manipulação de dados dos seus clientes, certifique-se que a plataforma é segura, e que tem o consentimento dos respectivos titulares - caso seja necessário. Garanta também que a finalidade da manipulação está adequada à sua necessidade, de acordo com o que determina a Lei Geral de Proteção de Dados.

A Credilink trabalha com dados para proteger pessoas e empresas, neste sentido disponibiliza um e-book gratuito apresentando maneiras de acessar dados respeitando a LGPD. Saiba mais clicando abaixo:

E-BOOK GRATUITO

Mantenha-se sempre atualizado sobre a segurança digital e adapte-se conforme as tendências de segurança na internet.

A Credilink Informações de Crédito possui mais de três décadas de experiência no mercado de dados para proteção ao crédito e prevenção de fraudes financeiras. Oferecemos informações seguras para proteger pessoas e empresas. Conheça clicando no botão ao lado.

ACESSE

O Peck Advogados tem mais de 20 anos de experiência em Direito Digital com atuação nacional e internacional. Para conhecer mais sobre o trabalho e a equipe do Peck Advogados, clique no botão ao lado.

ACESSE

O Instituto iStart foi criado em 2010 pela advogada especialista em Direito Digital, Dra. Patricia Peck Pinheiro, com o objetivo de difundir a educação em Ética e Segurança Digital entre as famílias brasileiras. Acompanhe as atividades do Instituto clicando no botão ao lado.

ACESSE

EXPEDIENTE

COORDENAÇÃO

Patricia Peck Pinheiro

AUTORES

Larissa C. Lotufo da Costa

Diago Savio M. de M. Sucar

Felipe Mury Botelho

COAUTORIA

Anna C. Leonetti do S. Janni

COLABORAÇÃO

Elisa Matos O. Fernandes

ILUSTRAÇÃO

Junior Meneguette

Freepik.com

PROJETO GRÁFICO

Diago Savio M. de M. Sucar

Felipe Mury Botelho

Junior Meneguette

Erik Getzel

DIAGRAMAÇÃO

Erik Getzel

REALIZAÇÃO

Credilink Informações de Crédito

iStart - Instituto Internet no Estado da Arte

Peck Advogados Associados

SEGURANÇA
NA INTERNET
A PRAÇA PÚBLICA VIRTUAL

iStart Ética Digital

Peck+ Advogados
Direito para Inovação Digital

CREDILINK®
INFORMAÇÕES DE CRÉDITO