SistemaOCB

inovacoop

MANUAL PRÁTICO DE segurança na internet

Tudo o que você precisa saber para prevenir você e a sua cooperativa de ataques e golpes virtuais

CONTEÚDOS

INTRODUÇÃO

Redes sociais, contas de e-mail pessoal e corporativa, *internet banking*, aplicativos para as mais diversas finalidades, *smartphones, smartwatches*, TVs e geladeiras inteligentes... a lista de interações virtuais que nos cerca é praticamente infinita e só tende a aumentar, já que o conceito de *IoT* (traduzindo-se em "internet das Coisas") está cada vez mais difundido, com objetos dos mais improváveis acessando a internet para transmitir e receber dados.

A internet se difundiu tanto e se tornou onipresente na vida das pessoas por causa de sua utilidade e capacidade de melhorar processos, otimizar tarefas, economizar tempo e recursos físicos, dentre outros benefícios. A internet possibilita o desenvolvimento de interações que seriam muito difíceis de acontecer sem sua existência. Por meio dela é possível, por exemplo, estabelecer conexão com pessoas que estão distantes, o que viabiliza, inclusive, o trabalho remoto, algo que ganhou extrema importância desde que o distanciamento social foi imposto como forma de controle da pandemia, em 2020.

Também vimos no último ano o crescimento acentuado do comércio virtual de itens e serviços diversos, cuja manutenção da atividade somente foi possível devido à popularização da internet. Dados da pesquisa Webshoppers 43, da Ebit/Nielsen e do Bexs Banco, indicam que o comércio eletrônico avançou 41% em 2020 em todo o mundo. Com isso, o faturamento atingido chegou a R$ 87,4 milhões, o que representa a maior alta em 13 anos. Em 2018, por exemplo, o crescimento do comércio online foi de 12% e, em 2019, de 16%.

Apesar de todas essas vantagens, dentre incontáveis outras, como em qualquer atividade humana, a internet também tem riscos inerentes. Em certo sentido, da mesma forma que a internet facilita a vida das pessoas, empresas e instituições, também cria uma série de possibilidades e oportunidades para pessoas mal-intencionadas. Ou seja, que vão tentar se aproveitar de brechas de segurança e da ingenuidade das pessoas para aplicar golpes.

É sobre os riscos existentes no uso da internet, os problemas mais comuns e também sobre como se precaver de golpes, que vamos falar ao longo deste e-book. Para isso, usamos como base os conteúdos das cartilhas do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil (CERT.br).

De fato, a prevenção é um assunto extremamente importante, pois os números de fraudes são tão elevados quanto os valores financeiros movimentados por meio da internet. Segundo a Apura Cybersecurity Intelligence, houve uma alta de 394% nas ameaças eletrônicas em 2020, chegando a 272 milhões de ameaças virtuais somente no Brasil. Somente em 2020, houve o vazamento de 958 mil CPFs, quase 950 mil cartões de crédito e mais de 220 milhões de senhas.

A mesma empresa afirma que há, no mundo, pelo menos, 15 gangues especializadas num tipo de golpe chamado *ransomware.* Na prática, os criminosos sequestram dados de pessoas físicas e empresas e exigem um resgate em dinheiro para devolver o acesso aos dados. Apenas com esse tipo de golpe a Apura (primeira empresa brasileira a participar da elaboração do principal relatório de investigação sobre vazamento de dados no mundo) estima que o lucro dos bandidos foi de mais de US$ 1 bilhão, em 2020.

É para evitar que esse tipo de problema atinja você e a sua cooperativa que neste material vamos falar sobre alguns conceitos e dicas extremamente importantes para quem usa a internet. Vamos abordar quais são os problemas mais comuns e trazer orientações valiosas para os usuários, mostrando como os golpes - e os prejuízos - podem ser evitados.

Além disso, na segunda parte deste material, vamos falar sobre os riscos existentes na internet sob o aspecto dos profissionais da área de TI das cooperativas. Assim, vamos mostrar quais são os pontos que merecem atenção especial por serem os mais vulneráveis e, portanto, passíveis de problemas relacionados a golpes na internet.

Conceitos importantes

Antes de entrar nas dicas, no entanto, é muito importante entender alguns dos principais conceitos relacionados à segurança. Vamos explicar, resumidamente, o que é privacidade e o que é a LGPD (Lei Geral de Proteção de Dados).

Privacidade

A cada dois anos a quantidade de dados dobra na internet, em média. Uma fatia bastante relevante deste volume é composta por informações pessoais. Afinal, usamos a internet para acessar bancos, trocar mensagens com amigos e familiares, trabalhar, comprar itens para a casa, contratar pacotes de viagem e até encontrar um par romântico.

Sem exceção, todas essas atividades só podem ser realizadas com o fornecimento de dados pessoais. E esta é a moeda mais valiosa do mundo digital. A existência de serviços online grátis como Facebook, Instagram e outras redes sociais somente é viável porque, em troca do uso, as pessoas concordam em ceder suas informações pessoais e dados relacionados a seus hábitos de navegação e consumo.

São dados valiosos para essas empresas, que os comercializam com empresas terceiras interessadas em atingir seus públicos-alvo. Faça um teste e pesquise por um produto ou serviço bastante específico no Google. Se suas contas de redes sociais e e-mails estiverem vinculadas - o que é mais do que usual -, você passará a receber constantemente conteúdos e ofertas relacionados à sua busca.

Isso não é por acaso. As empresas com ofertas relacionadas às suas buscas pagam para ter acesso aos dados de pessoas interessadas em seus produtos e serviços. Mas nem sempre as regras são claras e, mesmo quando são, em certos casos, se a pessoa não concordar com os (longos) Termos de Uso, que regulam o funcionamento de determinado site, ela fica limitada em sua utilização.

Em resumo, a Política de Privacidade de um site explica como são tratados os dados pessoais fornecidos pelo titular. Pode haver coleta de dados pessoais através do preenchimento voluntário de formulários, além de acompanhamento de navegação com rastreadores dos cliques realizados pelo usuário e por meio de *cookies,* por exemplo. Destes, o titular deve saber o que é necessário para o funcionamento do site e o que é opcional, possibilitando que escolha se os ativa ou não. Por isso, é importante que haja uma *pop-up* explicando essas opções, descrevendo para que servem, se houver, os *cookies* analíticos e os de marketing, e estando desativados por padrão.

Considere que, na prática, qualquer atividade *on-line* exige a troca de informações entre seu computador ou celular e um servidor, que muitas vezes está hospedado em outro país. Ao longo de todo esse percurso, é necessário garantir não só que a comunicação esteja segura, mas também que os dados coletados sejam informados ao titular e cheguem aos devidos destinatários, sem vazamentos.

POR ISSO, VAMOS A ALGUMAS
DICAS PARA PROTEGER A SUA PRIVACIDADE ONLINE.

E-mails

- Sempre use uma conexão segura para acessar seus e-mails em navegadores *Web,* pois isso evita que sejam interceptados;
- Para evitar roubo de senhas e acesso indevido a sua conta, evite usar computadores de terceiros, como *lan house*;
- Ao acessar o *webmail,* digite a *URL* diretamente no navegador;
- Tenha cuidado ao clicar em *links* recebidos por e-mail, sempre passe o *mouse* sobre o *link* e veja o endereço que é exibido – se não for conhecido, não clique em hipótese alguma;
- Caso use um programa específico para ler e-mails, prefira os que contam com recurso de criptografia, que aumenta a segurança de e-mails armazenados, reduzindo o risco de invasões;
- Não confie no conteúdo do e-mail, como *links* e documentos, só porque foi recebido de um remetente conhecido, pois ele pode ter sido vítima de *hacker*;
- Se não fez a solicitação da informação a ser recebida por e-mail, não confie no e-mail, por exemplo: atualização cadastral, nota fiscal, validação de senha etc.

Navegadores

- Dê preferência a sites em que você possa escolher se ativa ou não os *cookies* existentes no domínio e que lhe expliquem para que serve cada um deles;
- Dê preferência por usar a navegação anônima do navegador, o que possibilita que não seja gravada a navegação em sua máquina;
- Opte por navegadores que permitam acionar a configuração "*Do not track*", que bloqueia parcialmente o rastreamento de informações, preservando sua privacidade.

Redes sociais

- Redes sociais são como locais públicos, onde tudo o que é publicado pode ser visto por qualquer pessoa para sempre. Por isso, pense bem ao publicar algo para evitar arrependimentos ou mal-entendidos, pois é muito difícil reverter os danos e apagar todos os rastros após a publicação;
- Leia atentamente as opções de privacidade das redes sociais para tornar o seu perfil o mais restrito possível, mantendo suas informações apenas entre pessoas que você realmente conhece, mas lembre-se que, mesmo assim, isso não é garantia de respeito total à privacidade;
- Selecione bem os contatos que aceita em sua rede, pois quanto maior ela for, mais você e suas informações ficam expostos;

- Restrinja o acesso ao seu endereço de e-mail, pois há robôs na internet que capturam essa informação para disparar e-mail de spam;

- Muito cuidado com as informações que você consome e, principalmente, repassa. Afinal, há muitas informações falsas nas redes sociais, o que exige verificação da veracidade das informações em fontes confiáveis. Se você desconfiar de algo, pode checar diretamente em sites de credibilidade que fazem essa verificação, como a Agência Lupa e Aos Fatos, por exemplo;

- Seja criterioso ao seguir páginas que possam captar indícios sobre seus hábitos, rotinas e locais que frequenta, pois você não tem garantias se existem pessoas mal-intencionadas nessas redes;

- Evite fornecer sua localização exata, tomando cuidado com fundos de fotos e vídeos que possam revelar onde você está. Desative a captura de localização das fotos, salva em metadados, que são informações (hora, exposição etc.) sobre as fotos tiradas com o celular. Da mesma forma, não torne públicos seus planos de viagem ou seus períodos de ausência de casa. Se precisar ou quiser fazer check-in, faça quando estiver saindo do local e não quando chegar;

- Respeite a privacidade alheia, evitando divulgar imagens de outras pessoas sem autorização, mesmo que sejam suas amigas ou familiares. Também não divulgue informações que constam no perfil de pessoas da sua rede.

Informações de login e senha

- Elabore e use senhas fortes e diferentes para cada perfil social e conta. Evite usar a mesma senha somente com o final diferente, nomes de familiares, datas de nascimento, que são fáceis de serem descobertas;

- Habilite a autenticação em duas etapas e as notificações de login, que informam por SMS ou e-mail quando alguém acessar sua conta;

- Sempre faça o *logout* ao terminar de usar sua conta. Ou seja, clique na opção “sair” e confirme.

LGPD (Lei Geral de Proteção de Dados)

A LGPD, em vigor desde 18 de setembro de 2021, inaugura um microssistema jurídico específico para o estabelecimento de garantias, direitos e deveres relacionados às atividades diversas que envolvem a utilização de dados pessoais (dados de pessoa física), inclusive na internet.

O objetivo da LGPD é garantir que todas as pessoas físicas (denominadas, segundo a lei, como titulares de dados pessoais) estejam bem informadas sobre os propósitos para os quais os seus dados pessoais são utilizados, que possam responsabilizar aquelas organizações que os utilizam indevidamente e, ainda, que estejam na posição de decidir, em algumas situações, quando seus dados pessoais podem ou não ser utilizados para determinadas finalidades.

A LGPD pretende inaugurar tempos mais sinérgicos entre valores importantes para as pessoas físicas, tais como privacidade e liberdade de escolha e necessidades das organizações (cooperativas, empresas, órgãos públicos etc.) que desenvolvem determinadas atividades com dados pessoais. Para tanto, a lei estabelece uma série de valores gerais (princípios), diretrizes e boas práticas que devem ser observadas pelas organizações que utilizam dados pessoais nos seus mais variados processos de negócios, tal como é o caso das cooperativas.

DENTRE TAIS VALORES E DIRETRIZES, DESTACAM-SE OS 10 PRINCÍPIOS ESTABELECIDOS PELA LGPD:

1. Finalidade específica e informada explicitamente ao titular
2. Adequação à finalidade previamente acordada e divulgada
3. Necessidade do tratamento, limitado ao uso de dados essenciais para alcançar a finalidade inicial
4. Acesso livre, fácil e gratuito das pessoas à forma como seus dados são tratados
5. Qualidade dos dados, deixando-os exatos e atualizados, segundo a real necessidade
6. Transparência, ao titular, com informações claras e acessíveis sobre o tratamento e seus responsáveis
7. Segurança para coibir situações acidentais ou ilícitas como invasão, destruição, perda, difusão

8 Prevenção contra danos ao titular e a demais envolvidos

9 Não discriminação, ou seja, não permitir atos ilícitos ou abusivos

10 Responsabilização do agente, obrigado a demonstrar a eficácia das medidas adotadas

Observação: Este material não tem a intenção de esgotar o tema sobre proteção de dados pessoais.
É interessante que usuários de internet busquem conhecimento sobre seus direitos com relação às interações que estabelecem na internet, bem como que as cooperativas busquem medidas para adequação e segurança dos seus ambientes virtuais. Para saber mais sobre o assunto, acesse o e-book "LGPD no cooperativismo: como se adaptar", disponível no portal InovaCoop.

Lei de crimes cibernéticos

Após o vazamento de fotos íntimas da atriz Carolina Dieckmann, em 2012, vários movimentos se mobilizaram e apoiaram iniciativas para criação de uma lei que alterasse o Código Penal para possibilitar o adequado processamento e punibilidade de crimes ocorridos em meio virtual. Como resultado de tais movimentos, foi aprovada a Lei 12.737/2012, que alterou o Código Penal brasileiro.

OS ARTIGOS ACRESCIDOS AO CÓDIGO FORAM OS SEGUINTES:

Artigo 154-A: trata da invasão de dispositivo informático, que foi o caso da atriz cujo nome foi associado à lei;

Artigo 154-B: regulamenta a ação penal em si, determinando a necessidade de representação legal;

Artigo 266: trata de crimes relacionados à interrupção ou perturbação de serviços telegráficos, telefônicos, informáticos, telemáticos ou de informação de utilidade pública;

Artigo 298: aborda a questão da falsificação de documentos particulares, como cartões de crédito e débito.

Mais uma vez, é interessante que o usuário da internet conheça minimamente a lei de crimes digitais, a chamada Lei Carolina Dieckmann, para entender quais são seus direitos e deveres e em quais casos deve acionar a Justiça devido a crimes envolvendo dispositivos eletrônicos e a internet.

Uso seguro da internet

Imagine a seguinte situação: Cris é uma pessoa que tem muito dinheiro, ganho com muito trabalho honesto e que gosta de ostentar onde quer que seja. Por isso, anda pela grande cidade onde reside com um relógio caro e vistoso à mostra, usa apenas roupas e calçados de marcas de luxo, anda com um carro novo cujo valor ultrapassa as centenas de milhares de reais. Cris não se preocupa com discrição ou segurança, chegando a deixar o carro aberto com seu smartphone de última geração dentro enquanto vai ao banco sacar elevadas quantias.

Não é difícil imaginar que, numa situação dessas, Cris seria vítima fácil de assalto ou sequestro, concorda?
Tudo porque não se preocupa em manter um padrão mínimo de segurança e por não achar que, dentre tantas pessoas numa cidade, algo de ruim justamente lhe aconteceria.
Se parece absurdo pensar dessa maneira na chamada vida física, por que seria diferente na vida virtual?

Essa é, possivelmente, a origem mais comum dos problemas ocorridos na internet, a sensação de que, com tantas pessoas conectadas, você não seria alvo de ações de criminosos. Por que algo aconteceria comigo entre bilhões de pessoas? É um pensamento equivocado, pois os criminosos contam com sistemas sofisticados que testam a segurança de milhares de computadores por dia até encontrar brechas a serem exploradas. Dessa maneira, o primeiro passo é entender que o mundo virtual é apenas uma representação do mundo real. Ou seja, há possíveis criminosos à espreita esperando oportunidades de atacar e as ações na internet levam a consequências reais.

O ideal, portanto, é adotar uma postura preventiva, incorporando a preocupação com segurança às ações diárias na internet. Uma maneira prática de fazer isso é adotando mecanismos e procedimentos de segurança, senhas seguras e criptografia. Vamos falar mais detalhadamente sobre isso adiante. Por enquanto, vamos pontuar algumas atitudes simples para fazer o uso seguro da internet.

Acesso a conteúdos impróprios ou ofensivos

Infelizmente, a navegação na internet está sujeita à exposição a conteúdos impróprios, com pornografia, que incitam discursos de ódio ou atentam contra a honra das pessoas. Para reduzir o risco de exposição a esse tipo de conteúdo é necessário atentar para a confiabilidade dos sites visitados, dando preferência por aqueles com qualidade assegurada e políticas de segurança e privacidade bem estabelecidas.

Contato com pessoas mal-intencionadas

A internet passa uma falsa sensação de anonimato, de que não há ninguém vendo o que está sendo feito. Logo, algumas pessoas se aproveitam disso para aplicar golpes e cometer crimes, além de ofender e expor outras pessoas. É preciso cuidado, especialmente nas redes sociais, com pessoas com comportamento estranho ou ofensivo. Caso note alguma atitude pouco usual por parte de alguém que você conhece, procure saber se realmente está falando com a pessoa correta. Se apropriar indevidamente de perfis no Facebook ou contas no WhatsApp estão cada vez mais comuns. Por isso, sempre desconfie de um conhecido pedindo dinheiro, se ele não tem o costume de realizar este pedido, já que isso é um forte indício que a pessoa está sendo vítima de um ilícito.

Apropriação de identidade e perda de dados pessoais

Um criminoso toma o acesso de suas redes sociais e/ou aplicativos para tentar extorquir pessoas que você conhece. Para reduzir esse risco, adote senhas fortes, ative a autenticação em dois fatores e procure não expor muito da sua vida na internet.

Invasão de privacidade

O compartilhamento de informações pessoais sem base legal adequada - a LGPD estabelece que as atividades de tratamento de dados pessoais, dentre as quais o compartilhamento, devem ser realizadas apenas mediante o enquadramento em alguma das hipóteses legais indicadas em lei - pode comprometer a privacidade e a segurança. Uma vez que estão na internet é muito difícil - para não dizer impossível - reverter sua divulgação. Logo, seja muito criterioso ao divulgar dados pessoais, evitando ao máximo publicar informações sem necessidade e, quando o fizer, optando por sites com credibilidade.

Divulgação de boatos

Nos últimos anos o debate político ganhou o mundo virtual. Com discussões cada vez mais acirradas, entrou em campo um ator poderoso: o boato, também conhecido como *fake news*. Esse elemento sempre existiu e continuará existindo, mas a internet foi capaz de amplificar seu impacto em níveis globais. Por isso, é preciso muito cuidado e critério com relação às informações consumidas e, principalmente, verificar a autenticidade delas antes de repassar. Procure se informar a partir de fontes confiáveis, como jornais críveis, e evite consumir notícias de apenas uma única fonte. Aproveite a diversidade proporcionada pela internet para obter diferentes pontos de vista sobre os assuntos que lhe interessam e formar uma opinião mais fundamentada e rica. Da mesma maneira, evite propagar informações que não agregam às pessoas que leem e que podem causar preocupação ou prejudicar outras pessoas.

Evite danos com o que você fala

Uma ofensa ou resposta grosseira num momento de irritação em família ou mesmo no trabalho pode causar prejuízos, não é mesmo? No entanto, se for um ponto fora da curva no seu comportamento padrão, uma conversa franca e desculpas sinceras podem reverter ou, no mínimo, controlar a situação.

Na internet é um pouco diferente, pois opiniões controversas ficam sujeitas a uma possibilidade de disseminação virtualmente infinita. E sem o devido contexto, o que pode piorar ainda mais as coisas. Então, prudência, equilíbrio e boa educação são, provavelmente, os ingredientes mais importantes ao emitir opiniões na internet para que elas não se tornem um problema para você.

Impessoalidade

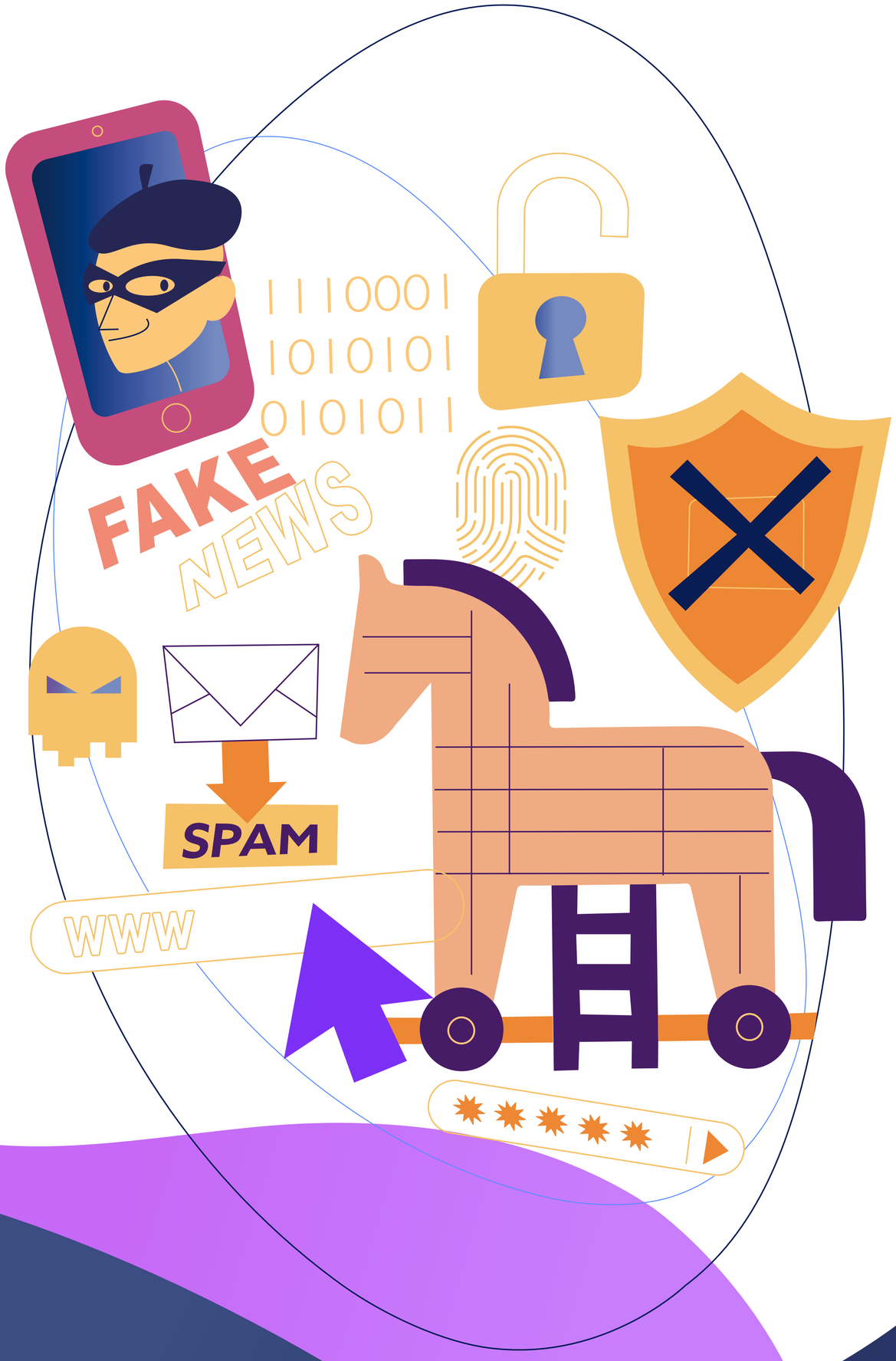
Por meio da comunicação virtual é muito difícil detectar e expressar sentimentos. A impossibilidade de observar expressões faciais, o posicionamento do corpo e o tom da voz são fontes ricas para o surgimento de mal-entendidos e interpretações incorretas. Por isso, a comunicação pela internet exige muito mais clareza, incluindo explicar o que pode parecer óbvio.

Uso excessivo

Da mesma forma que a internet é um recurso valioso para o trabalho, os estudos e a vida social, pode se tornar um problema caso seu uso seja desmedido. O aumento do surgimento de problemas de postura e psicológicos estão associados ao tempo excessivo de tela, bem como questões de produtividade e desempenho. É imprescindível manter vigilância constante acerca da quantidade de tempo despendido na internet, pois redes sociais contam com engenharia sofisticada para reter a atenção das pessoas pelo máximo de tempo possível.

Plágio e violação de direitos autorais

Por trazer uma facilidade até então impensável para disseminação e reprodução de materiais, a internet também é campo fértil para plágios e violação de direitos autorais. Ao compartilhar informações, sempre cite a fonte e não retransmita a ninguém conteúdos que não tenham sido disponibilizados de maneira gratuita.



Riscos mais comuns

Agora que já falamos sobre como se portar na internet para reduzir o risco de exposição, é importante citarmos alguns dos riscos mais comuns para quem trafega no ambiente virtual. Afinal, por mais que cada vez mais tecnologia seja utilizada para que criminosos obtenham vantagens indevidas na internet, os mecanismos de atuação costumam compartilhar algumas semelhanças. Ou seja, ter um mínimo de conhecimento sobre como os golpes e ataques se desenrolam ajuda a evitar a maior parte dos problemas.

Golpes

Bancos e grandes empresas investem pesado em tecnologia para aumentar a segurança de seus sites e sistemas virtuais. Por isso, a maior parte dos golpes e ataques se volta contra usuários comuns, que apresentam mais fragilidades e vulnerabilidades.

Até mesmo porque nem sempre é necessário para os criminosos contar com recursos tecnológicos para dar golpes. Em muitos dos casos, o que acontece é uma migração do antigo malandro, que aplicava golpes na praça, para o ambiente virtual. Esses criminosos criam situações para enganar e persuadir as vítimas a fornecer informações e realizar ações, como abrir arquivos danosos ou acessar páginas que coletam dados indevidamente.

Depois, com os dados em mãos, começam a realizar transações financeiras, enviar mensagens para a lista de contatos pedindo dinheiro, dentre diversas outras ações danosas. Em geral, os criminosos cometem crimes de estelionato e contra o patrimônio das vítimas.

OS GOLPES MAIS COMUNS SÃO:

Apropriação de identidade: seus dados pessoais podem ser usados para criar perfis falsos e até mesmo para abrir empresas.
A melhor forma de impedir esse tipo de golpe é dificultando, em várias etapas, o acesso aos seus dados e às suas contas de usuário, além de usar senhas fortes e seguras, e fique atento aos seguintes indícios:

- Problemas com órgãos de proteção ao crédito;
- Recebimento do retorno de e-mails que não foram enviados por você;
- Notificações de acesso a contas de e-mail ou perfis em redes sociais em horários ou locais em que você próprio não estava acessando;
- Transações que não foram realizadas por você no seu extrato bancário;
- Ligações telefônicas, correspondências e e-mails relacionados a assuntos sobre os quais você não sabe nada a respeito.

Fraude de antecipação de recursos: nesse golpe, o criminoso promete uma vantagem futura muito expressiva em troca de um pagamento adiantado. Geralmente envolve uma história mirabolante, como o famoso Golpe da Nigéria. Nesta história, alguém se passa por representante de uma instituição nigeriana e afirma ter um montante gigantesco de dinheiro bloqueado por algum imprevisto jurídico. Em seguida, o criminoso pede ajuda para arcar com os custos com advogados necessários para liberar a quantia em troca de uma porcentagem expressiva do valor bloqueado. Algumas vítimas, interessadas na suposta vantagem financeira, transferem quantias que nunca mais são recuperadas, assim como a recompensa final prometida nunca é paga. Para evitar este golpe é importante refletir sobre o porquê, dentre todas as pessoas que poderiam ser acionadas no planeta para resolver esse suposto problema, você foi o escolhido. Além disso, seja na internet ou pessoalmente, a antecipação de recursos como promessa de recompensa futura é, em geral, indício de golpe. É importante, ainda, lembrar que existem inúmeras variações dessa história, todas com mecanismo similar, como:

- Oferta de quantias absurdas de dinheiro;
- Exigência por sigilo absoluto nas transações;
- Resposta imediata sob risco de perder a oportunidade;
- Presença de palavras de urgência no assunto;
- Erros de gramática e ortografia decorrentes da tradução automática.

Comércio eletrônico: existem variações do golpe de comércio eletrônico, mas, em geral, o mecanismo é o mesmo. Os golpistas criam uma oferta fictícia extremamente atraente, como preços muito baixos ou condições de pagamento imperdíveis, e exigem uma resposta rápida por parte das vítimas. Para tanto, é usual afirmarem que há poucas unidades ou que o tempo está esgotando, sempre de forma a fazer com que as pessoas tomem decisões por impulso e não percebam o golpe. É preciso muita atenção nesses casos porque, por vezes, os golpistas simulam até mesmo o ambiente (com a mesma identidade visual de cores, logos etc.) de um site confiável, como o de um grande varejista, para dar a sensação de segurança. Algumas dicas para evitar esse tipo de problema são:

- Fazer pesquisas de mercado para verificar a média de preço do produto oferecido e desconfiar caso o valor esteja muito abaixo da média;
- Não se submeter à pressão por tempo ou escassez de produtos;
- Ficar desconfiado de ofertas recebidas por e-mail, links patrocinados ou por aplicativos de mensagens;
- Não realizar transações financeiras em sites sem certificado de segurança (na barra de endereço do site é possível identificar se o endereço possui “https”);
- Antes de efetuar a compra verifique a idoneidade do site e sua reputação. Você pode fazer isso em sites como o Reclame Aqui;
- O Web of Trust (WOT) também é um ótimo meio de analisar a reputação de uma loja virtual. Ao fazer uma busca por determinado site, ele exibe a média das notas atribuídas pelos usuários em quesitos como confiança, privacidade e conteúdo para crianças.

Ataques

Qualquer dispositivo conectado à internet está sujeito a ataques, que podem ter como motivação desde a necessidade de demonstração de poder por parte do hacker, questões ideológicas, comerciais ou, é claro, financeiras. Para realizar esses ataques, os criminosos costumam explorar as seguintes possibilidades:

Vulnerabilidades: falhas nos sistemas que permitem ações maliciosas, como acesso a informações confidenciais e bloqueios de acesso, dentre outros;

Varreduras em redes: buscas minuciosas em redes de computadores para coletar informações;

Falsificação de e-mail: alteração de campos do cabeçalho de um e-mail para dar a entender que foi enviado por uma fonte confiável quando, na verdade, foi disparado por um golpista. Nesses casos, costumam ser e-mails supostamente de pessoas ou instituições conhecidas, mas que pedem para clicar em links ou abrir anexos suspeitos, solicitam dados bancários ou informações pessoais;

Força bruta: apesar do nome, esse golpe não envolve agressões físicas. Se trata, na verdade, de sistemas capazes de testar milhões de combinações de senhas até conseguir acessar uma conta. Nem sempre o interesse do golpista está em entrar na conta, mas em bloquear seu acesso, fazendo com que a vítima busque alternativas para recuperar o acesso e, assim, venha a cair no golpe;

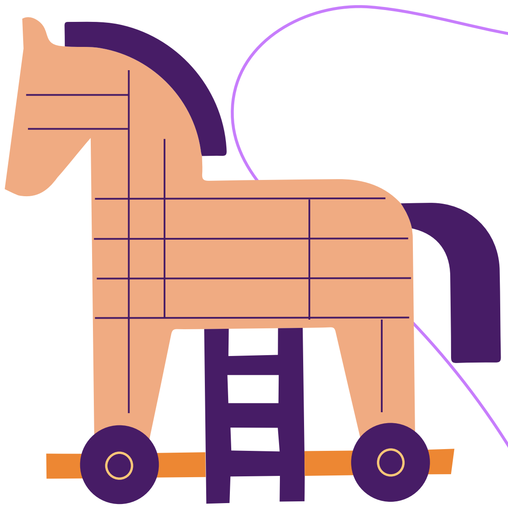
A prevenção para todos esses ataques está no uso de mecanismos de segurança, como antivírus, no uso de senhas fortes e de criptografia.

Malwares

Toda e qualquer página de internet, aplicativo ou programa de computador tem um código de programação por trás. Criminosos usam do mesmo princípio para invadir computadores. São os chamados códigos maliciosos, ou *malwares*. Para fazer com que um computador ou dispositivo móvel execute *malwares*, os criminosos costumam explorar vulnerabilidades dos sistemas, utilizar portas de entrada, como *pen drives* ou sites maliciosos, ou por meio da execução de arquivos infectados enviados por e-mail.

Quando instalados, os *malwares* acessam os dados armazenados e executam ações prejudiciais aos usuários. Os principais tipos de *malwares* são:

- Vírus
- *Worm*
- *Bot e Botnet*
- *Spyware*
- *Backdoor*
- Cavalo de Troia *(Trojan)*
- *Rootkit*



Cada um deles age de uma maneira específica. O importante, para se prevenir desse tipo de problema, é manter seu computador ou dispositivo móvel atualizado quanto à versão mais recente de seu sistema operacional, além de usar mecanismos de segurança, como antivírus, *antimalwares e firewalls.*

Ransomwares

O *ransomware* é uma modalidade de ataque que utiliza *malware* e exige recompensa para restaurar a disponibilidade das bases de dados do computador ou dos computadores da vítima, tornando inacessível (por exemplo, por criptografia) as bases de dados até que haja pagamento de resgate. Via de regra, o sistema operacional do (s) usuário (s) é codificado, impedindo seu acesso – demandando, na maioria das vezes, especialmente no contexto corporativo, a restauração dos ambientes através de backup.

As Diretrizes 01/2021 do *European Data Protection Board* trazem um bom exemplo de incidente envolvendo ataque de *ransomware*:

> O servidor de uma empresa de transporte público foi exposto a um ataque de ransomware e seus dados foram criptografados. De acordo com as conclusões da investigação interna, o perpetrador não só criptografou os dados, mas também os exfiltrou (...) violados foram os dados pessoais de clientes e funcionários, e das várias milhares de pessoas que usam os serviços da empresa (...) Além dos dados básicos de identidade, números de carteira de identidade e dados financeiros, como detalhes do cartão de crédito estão envolvidos na violação. Existia um banco de dados de backup, mas também estava criptografado pelo atacante."

Atualmente, é bastante comum que organizações vivenciem incidentes vinculados à infecção por *ransonware*, que, geralmente, utilizam como porta de entrada técnicas de *phishing* (entenda o que é no item abaixo), sites maliciosos, downloads de anexos remetidos por e-mails desconhecidos ou, ainda, cliques em links também remetidos por e-mails desconhecidos. É essencial, portanto, que além de medidas de proteção de rede, antivírus, firewall, entre outras, as cooperativas conscientizem os usuários sobre cuidados básicos, como não abrir links ou anexos remetidos por e-mails suspeitos e desconhecidos.

Conforme pesquisa conduzida pela organização Sophos em janeiro e fevereiro de 2021, a média de resgate pago pelas organizações de médio porte foi US$ 170.404,00, porém apenas 65% dos dados criptografados foram recuperados após o pagamento do resgate. Ou seja, o pagamento de resgate não dá certeza de que os dados sejam recuperados, somente de enriquecimento ilícito do atacante.

A mesma pesquisa citada acima traz um indicativo extremamente importante: 38% dos ataques de *ransomware* do mundo ocorreram no Brasil. Portanto, implementar medidas de segurança e de conscientização sobre o tema é essencial. No capítulo 4 deste e-book indicamos algumas das medidas que podem ser implementadas.

Spam

Lembra o que dissemos sobre o mundo virtual ser uma representação do mundo real? Pois essa afirmação vale também para esse caso. Em algum momento você já deve ter recebido na sua caixa de correio correspondências com oferta de produtos e serviços diversos, sem ter solicitado tal informação, certo? A forma virtual desse tipo de abordagem comercial é o Spam.

A grande diferença para quem envia Spam é a facilidade e o custo baixíssimo. Por que são considerados riscos à segurança? Porque nem sempre o Spam é apenas uma oferta legítima de um produto ou serviço. Por vezes, o e-mail não solicitado (Spam) traz um link ou arquivo malicioso e que pode causar danos ao seu computador, roubar informações confidenciais como usuários e senhas.

Além disso, como são enviados em grande quantidade, podem fazer com que você deixe passar mensagens realmente importantes ou, até mesmo, consumam todo o espaço de sua caixa de mensagens.

A maior parte dos serviços de e-mail já conta com mecanismos de prevenção ao Spam, direcionando esse tipo de mensagem para pastas específicas de lixo eletrônico. Esses mecanismos não são infalíveis, o que pode fazer com que alguns e-mails inconvenientes ainda venham a parar na sua caixa de mensagens. Para identificá-los, desconfie de:

- Cabeçalhos suspeitos, incompletos ou com cumprimentos genéricos;
- Palavras com grafia errada ou apelativas no campo “Assunto”;
- Assuntos alarmantes ou vagos;
- Ausência de opção de descadastramento;
- Solicitação de dados confidenciais como informações bancárias, usuários e senhas;
- Promoções imperdíveis.

Além disso, sempre clique na opção “Spam” do seu serviço de e-mail ao identificar uma mensagem desse tipo que passou pelo filtro automático do servidor. Isso “ensina” o servidor a identificar esse tipo de mensagem no futuro e impedir a propagação dos mesmos.

Phishing

O termo *phishing* deriva de *fishing*, que, por sua vez, significa pescaria. Isso porque se trata de um tipo de golpe em que os criminosos espalham iscas pela internet à espera de uma presa. É uma combinação de recursos técnicos com engenharia social que recorre ao envio de mensagens eletrônicas que:

- Simulam comunicações oficiais de empresas sérias, como bancos e lojas virtuais;
- Atraem a atenção das pessoas por curiosidade, caridade, assuntos que estão na moda ou possibilidade de obter vantagens financeiras;
- Causam alarme quanto ao bloqueio ou suspensão de algum serviço, devido ao não fornecimento ou atualização de informações. Essas atualizações normalmente solicitam a informação de senha;
- Induzem o usuário a acreditar que determinada página é real quando, na verdade, é uma cópia repleta de códigos maliciosos que coletam informações sensíveis.

Assim, na prática, o *phishing* é realizado por meio de:

- Páginas falsas de comércio eletrônico ou Internet Banking;
- Páginas falsas de redes sociais ou de companhias aéreas;
- Mensagens contendo formulários;
- Mensagens contendo links para códigos maliciosos;
- Solicitação de recadastramento.

Para se prevenir, é importante:

- Desconfiar de mensagens de instituições e empresas que solicitam informações, instalação de programas ou clique em links;
- Procurar entender por qual motivo uma empresa com a qual você não tem relação - como um banco onde você não tem conta - está enviando mensagens (e-mail, WhatsApp, SMS etc.) e solicitando atualização de cadastro;
- Ficar atento a mensagens alarmistas, que usam recursos apelativos para chamar a atenção, incluindo ameaças;
- Desconfiar inclusive de mensagens supostamente enviadas por pessoas conhecidas, pois a conta remetente pode ter sido invadida;
- Ser cuidadoso ao acessar links, dando preferência por digitar o endereço diretamente na barra de endereços do navegador;
- Antes de clicar, repouse o cursor do mouse sobre o link e verifique qual é a página de destino. Jamais clique caso o endereço pareça suspeito;

- Use mecanismos de segurança nos seus dispositivos eletrônicos;
- Acesse a página da instituição que supostamente enviou a mensagem e procure por informações. Na maior parte dos casos, as empresas sérias informam que não têm como política enviar mensagens com as características acima;
- As empresas sempre reforçam que não solicitam através de seus atendentes, mensagens ou e-mail que o usuário informe sua senha ou dados pessoais.

Outros riscos

Além dos riscos citados acima, os usuários de internet estão suscetíveis a outros tipos de ameaças causadas por pessoas mal-intencionadas. Seria impossível abordar todos nesse material, mas vamos listar as mais comuns:

- **Cookies:** são recursos legítimos utilizados por sites para monitorar o padrão de navegação dos usuários. É por causa dos cookies que os sites de comércio eletrônico conseguem lembrar do que estava no seu carrinho de compras na última visita à página. Entretanto, é claro que esse recurso é utilizado para finalidades maliciosas, como coleta indevida de informações pessoais. Como não é indicado bloquear totalmente o recebimento de cookies para evitar mal funcionamento de sites diversos, configure seu navegador para não receber cookies automaticamente;

- **Pop-ups:** são aquelas janelas que aparecem automaticamente em sobreposição à janela do navegador. Dentre os riscos que podem representar estão a exposição a conteúdos indesejados ou impróprios e links maliciosos. Para se prevenir, configure o navegador para bloquear esse tipo de recurso;

- **Plugins, complementos e extensões:** proporcionam funcionalidades extra ao navegador e, muitas vezes, são desenvolvidos por empresas terceiras. Grande parte desses recursos é confiável, pois foi selecionada pelo próprio desenvolvedor do navegador antes de ser oferecido. No entanto, é sempre útil atentar para a quantidade de usuários que já os utilizam - quanto mais, melhor - e à avaliação média na loja do navegador. Além disso, verifique se as solicitações de autorização são coerentes com o uso. Um complemento que oferece um corretor ortográfico, por exemplo, não precisa ter acesso às suas fotos, gerenciar e fazer ligações telefônicas e acesso aos contatos;

- **Links patrocinados:** às vezes você procura por uma empresa em específico na internet e o primeiro resultado de busca é de uma empresa concorrente. Já notou isso? São os chamados links patrocinados. Ou seja, a empresa concorrente pagou para aparecer na primeira posição. Muitas vezes, se trata apenas de um concorrente mesmo. No entanto, alguns golpistas compram a primeira posição para direcionar os usuários para páginas maliciosas, que roubam dados. Por isso, antes de clicar pare o cursor do mouse sobre o link e verifique, no canto inferior esquerdo do navegador, se o endereço de destino é mesmo o que você está buscando. Nunca clique em endereços que por qualquer motivo pareçam suspeitos;

- **Banners de propaganda:** mais uma vez, criminosos exploram a boa-fé das pessoas, anunciando produtos e serviços que não existem como forma de obter dados pessoais. Ao ser exposto a uma publicidade na internet, desconfie sempre do conteúdo. Especialmente se apresentar vantagens demais ou solicitar informações ou pagamento para apresentar a oferta;

- **Compartilhamento de arquivos:** é bastante comum usar a internet para compartilhar arquivos de música, apostilas, livros, filmes etc. Por isso, esse é um dos caminhos mais explorados por criminosos para invadir computadores. Para evitar isso, mantenha os programas de compartilhamento e proteção sempre atualizados e tenha certeza de que os arquivos distribuídos são de livre acesso para não incorrer no risco de cometer crimes contra direitos autorais.

Dicas e melhores práticas

Caso além de usuário de internet você seja também um dos profissionais responsáveis pelo acesso e segurança de rede da sua cooperativa, precisa tomar alguns cuidados extras. É sobre esse aspecto da segurança na internet que vamos falar a partir de agora. Recomendamos que os tópicos a seguir sejam lidos por todos, inclusive usuários, pois as informações certamente vão colaborar para um melhor entendimento sobre a segurança na internet.

Mecanismos de segurança

Para solicitar seus dados, um site precisa se mostrar confiável. E isso é feito por meio de alguns dispositivos de segurança. É como solicitar os documentos de uma pessoa para comprovar que não ocorra uma fraude de roubo de identidade. Os principais mecanismos de segurança que sites devem elaborar e disponibilizar são:

- **Política de segurança:** define direitos e responsabilidades das partes - empresa responsável pelo site e usuários - quanto à segurança. Esse documento esclarece qual é o comportamento esperado de cada um, além das consequências por seu não cumprimento. Dentre as políticas de segurança mais importantes estão: política de senhas, política de backup, política de privacidade, política de confidencialidade e política de uso aceitável (PUA). Ao elaborar cada uma dessas políticas, os profissionais de TI precisam ter em mente qual é o posicionamento da cooperativa com relação aos temas e, pelo mesmo motivo, é importante promover a atualização dos termos de tempos em tempos;

- **Notificação de incidentes e abusos:** eventos não esperados que envolvam a segurança dos sistemas precisam gerar alerta para o usuário e para os responsáveis pelo sistema. Esse tipo de atitude contribui para a segurança global da internet, evitando que malwares contaminem outras redes, por exemplo. Uma notificação dessa natureza deve conter informações como: log completo; data, horário e fuso horário dos logs; e-mail completo; dados completos do incidente e informações relevantes;

- **Contas e senhas:** ao criar e disponibilizar sistemas, o time de TI deve exigir o uso de senhas fortes, contendo números, caracteres especiais, letras maiúsculas e minúsculas;

- **Backups:** as cópias de segurança são a garantia de que dados importantes serão preservados no caso de os sistemas enfrentarem problemas. A realização de backups periódicos proporciona proteção de dados, permite a recuperação de versões e o arquivamento de informações importantes. Assim, o profissional de TI deve sempre manter os backups organizados, atualizados e armazenados em local seguro;

- **Logs:** nada mais são do que o registro de eventos. Um log é a gravação de todas as atividades realizadas por um sistema e que permite identificar o uso indevido da rede, detectar ataques, rastrear atividades suspeitas e diagnosticar problemas. Para tanto, é importante garantir que o sistema esteja com o horário atualizado, que há espaço suficiente no disco rígido e que não estão sendo registrados dados desnecessários. Além disso, é recomendável restringir o acesso aos logs como forma de preservar evidências no caso de problemas;

- **Ferramentas antimalware:** conhecidas mais popularmente como antivírus, detectam, anulam e removem códigos maliciosos dos sistemas. É comum que as ferramentas disponíveis ofereçam, ainda, outras funcionalidades, como geração de discos de emergência e firewall. O ideal é que o antimalware seja configurado para verificar automaticamente arquivos anexados a e-mails e a pen drives;

- **Firewall:** a tradução de firewall é “parede de fogo”, o que remete a uma barreira intransponível para invasores. Assim, o firewall registra as tentativas de acesso ao computador, bloqueia o envio de informações coletadas por códigos maliciosos, impede o acesso por meio de vulnerabilidades do sistema e analisa continuamente o conteúdo das conexões online. Para garantir que funcione adequadamente, é necessário que o firewall seja de boa procedência e que esteja sempre ativo e atualizado.

Contas e senhas

Contas - ou logins - são a identificação única de um usuário em um sistema. Assim, após informar essa identificação, é necessário proceder com a autenticação do usuário, o que se dá por três vias:

1. Aquilo que você é: ou seja, informações biométricas, como sua impressão digital;
2. Aquilo que você possui: como um cartão com senhas bancárias ou um dispositivo gerador de tokens;
3. Aquilo que você sabe: são perguntas de segurança ou senhas.

O uso conjunto desse trio aumenta a segurança dos seus sistemas. Informações biométricas e tokens costumam ser menos vulneráveis, mas senhas se tornam mais seguras a partir de algumas práticas, como:

- Proibição de senhas com sequências numéricas, uso de nomes, sobrenomes e dados pessoais, como datas de aniversário;
- Proibição de uso de sequências de teclado, como “qwerty”;
- Exigência pelo uso de grandes quantidades de caracteres alfanuméricos;
- Exigência de uso de caracteres especiais, como #*%;
- Exigência por letras maiúsculas e minúsculas;
- Solicitação de troca de senha de tempos em tempos;
- Proibição de reuso de senhas;
- Bloqueio do usuário quando forem realizadas um número X de tentativas de login.

Segurança de computadores

Ao gerenciar os computadores de uma cooperativa, os responsáveis pela TI devem assegurar que os sistemas utilizados estejam atualizados conforme as versões mais recentes disponíveis. Por isso, é recomendável configurar os softwares para buscar e instalar atualizações automaticamente. Além disso, a boa gestão da segurança de computadores recomenda remover programas que não são mais utilizados, assim como versões antigas de sistemas.

Não é preciso dizer que é imprescindível utilizar somente programas originais e com códigos de licença ativos e com pagamento em dia. Caso contrário, o sistema pode ficar sujeito a invasões.

Outro procedimento de segurança recomendado é a realização periódica - em períodos curtos de tempo - de backups. Isso evita que os dados sejam perdidos no caso de mal funcionamento de algum software ou hardware. Pelo mesmo motivo é interessante criar um disco de recuperação do sistema, que permite reverter atualizações no caso de acontecer algum imprevisto, como uma incompatibilidade entre versões dos sistemas instalados.

Os times de TI também são orientados a impedir a instalação de aplicativos desenvolvidos por terceiros por parte dos usuários. Isso deve ser feito por meio da definição de privilégios de administrador, acessíveis apenas por senha.

Por isso, vale lembrar que a maioria dos sistemas operacionais prevê a criação de três tipos de conta de usuário:

Administrador (admin): tem controle completo sobre o computador e pode criar, alterar, excluir contas, instalar programas de uso geral e modificar configurações que afetam outros usuários ou o sistema operacional em si;

Padrão (standard): concede privilégios suficientes para a grande maioria dos usuários, como configurações estéticas, de notificações, acesso a e-mails e a documentos, por exemplo;

Convidado (guest): para usuários eventuais, não conta com senha e restringe as possibilidades de uso, permitindo apenas acesso ao navegador de internet e a execução de programas já instalados. Ao término da sessão, todos os dados, informações e arquivos criados são apagados.

Segurança de redes wi-fi

O acesso à internet por meio de rede sem fio é muito conveniente e comum, mas apresenta alguns riscos que precisam ser administrados pela equipe de TI. Afinal, por não dependerem de conexão física entre os dispositivos, podem abrir brechas para invasões e roubo de dados.

Por isso, o departamento de TI das cooperativas precisa saber que existem mecanismos de segurança como:

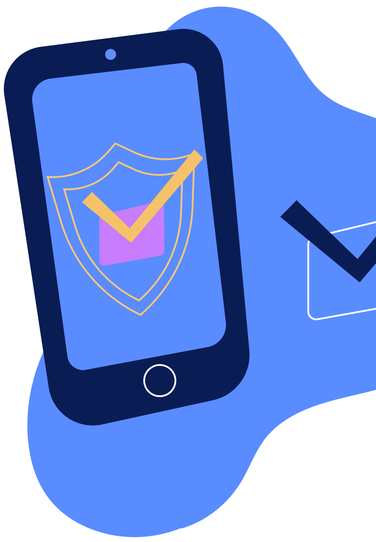
WEP (Wired Equivalent Privacy): primeiro mecanismo de segurança a ser lançado. É considerado frágil e, por isto, o uso deve ser evitado;

WPA (Wi-Fi Protected Access): mecanismo desenvolvido para resolver algumas das fragilidades do WEP. É o nível mínimo de segurança que é recomendado;

WPA-2: similar ao WPA, mas com criptografia considerada mais forte. É o mecanismo mais recomendado.

Além disso, é recomendado usar recursos de criptografia e autenticação nas redes e evitar o acesso a sites que não contam com conexão segura (https).

Segurança em dispositivos móveis



Os cuidados com este tipo de dispositivo são similares aos que devem ser tomados com computadores. Dentre eles, manter os sistemas sempre atualizados com a versão mais recente e a utilização de mecanismos de segurança.

Assim, se possível, é recomendável instalar um programa antivírus e tomar os devidos cuidados com a instalação de aplicações desenvolvidas por terceiros. Sempre prefira aplicações desenvolvidas por fontes confiáveis, com muitos usuários e boa avaliação nas lojas de aplicativos. Também evite usar aplicativos com geolocalização, pois isso expõe sua localização, podendo trazer riscos.

Da mesma forma, evite usar redes sem fio públicas, desabilite os recursos de bluetooth quando não estiver usando e faça backup dos seus dados periodicamente. Para evitar invasões ou códigos maliciosos, não siga links recebidos por meio de mensagens e use conexão segura sempre que a comunicação envolver a transmissão de dados sensíveis.

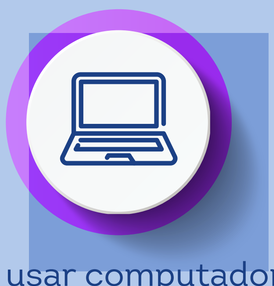
Resumo

Para facilitar a compreensão dos conteúdos apresentados neste e-book, criamos três quadros com as principais informações sobre segurança na internet, incluindo os riscos mais comuns e algumas dicas e melhores práticas para evitar problemas. Veja:

1 Utiliza a internet com frequência? **Proteja-se!**

Atividades online envolvem troca de informações, que podem vazar e comprometer sua privacidade. Dicas para se proteger:

Use conexão segura para acessar a internet

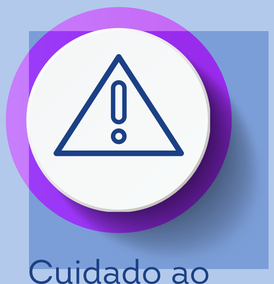


Evite usar computadores de terceiros

Digite a URL (endereço na rede) diretamente no navegador

Certifique-se se que o site que está visitando possui certificado de segurança válido

Cuidado ao clicar em links



Cuidado ao aceitar cookies

Dê preferência à navegação anônima do navegador

Pense bem ao publicar conteúdo nas redes sociais

Leia atentamente as opções de privacidade

Selecione bem os contatos com quem faz conexão

Seja criterioso ao seguir páginas que possam dar indícios sobre hábitos, rotinas e locais que frequenta

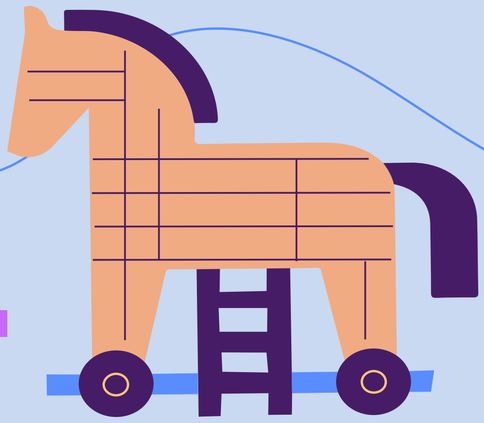
Evite fornecer sua localização

Respeite a privacidade alheia

Elabore e use senhas fortes

Habilite a autenticação em duas etapas e as notificações de login

Sempre faça o logout ao terminar de usar sua conta



2 Quais os riscos mais comuns?

Saber como golpes e ataques se desenrolam ajuda a evitar a maior parte dos problemas. Saiba mais sobre eles:

Golpes: estelionato cometido por criminosos que solicitam dados ou recursos financeiros em troca de produtos, serviços ou benefícios que não existem. Os mais comuns são:

- Furto de identidade
- Fraude de antecipação de recursos
- Comércio eletrônico falso

Ataques: criminosos exploram vulnerabilidades de sistemas para furtar dados ou dinheiro. A prevenção está no uso de mecanismos de segurança, como antivírus, no uso de senhas fortes e de criptografia.

Malwares: acessam dados e executam ações prejudiciais aos usuários. Para se prevenir, mantenha seu computador ou dispositivo móvel atualizado quanto à versão mais recente e use mecanismos de segurança, como antimalwares e firewalls.

Spam: envio de mensagens não solicitadas, que podem entupir sua caixa de entrada, levando à perda de informações importantes, além de trazer links maliciosos. Para evitar, desconfie de:

- Cabeçalhos suspeitos, incompletos ou com cumprimentos genéricos;
- Palavras com grafia errada ou apelativas no campo “Assunto”;
- Assuntos alarmantes ou vagos;
- Ausência de opção de descadastramento;
- Promoções imperdíveis.

Phishing: combinação de recursos técnicos com engenharia social que simulam comunicações oficiais para atrair a atenção das pessoas e as induz a fornecer informações sensíveis. Sempre desconfie de e-mails que solicitam informações, instalação de programas ou clique em links e fique atento a mensagens alarmistas, que usam recursos apelativos para chamar a atenção, incluindo ameaças.

Cookies: quando usado finalidades maliciosas, como coleta indevida de informações pessoais, é prejudicial. Por isso, configure seu navegador para não receber cookies automaticamente.

Pop-ups: podem expor os usuários a conteúdos indesejados ou impróprios e links maliciosos. Para se prevenir, configure o navegador para bloqueá-los.

Plugins, complementos e extensões: antes de instalar, confira a quantidade de usuários que os utilizam - quanto mais, melhor - e a avaliação média na loja do navegador, além de verificar se as solicitações de autorização são coerentes com o uso.

FAKE NEWS

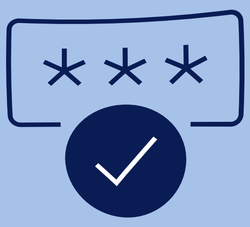
Links patrocinados: alguns golpistas compram a primeira posição de mecanismos de busca para direcionar usuários a páginas maliciosas, que roubam dados. Antes de clicar pare o cursor do mouse sobre o link e verifique se o endereço de destino é o que você está buscando e nunca clique em endereços suspeitos.

3 Qual o papel da TI?

Profissionais responsáveis pelo acesso e segurança de rede precisam tomar alguns cuidados extras e conhecer mais sobre:

Mecanismos de segurança: asseguram a autenticidade e confiabilidade de um site. Os mais comuns são:

- Política de segurança
- Notificação de incidentes e abusos
- Contas e senhas
- Backups
- Logs
- Ferramentas antimalware
- Firewall



Contas e senhas:
a identificação única de um usuário em um sistema envolve sua autenticação, que se dá por três vias:

- Aquilo que você é: informações biométricas;
- Aquilo que você possui: cartão com senhas bancárias ou tokens;
- Aquilo que você sabe: perguntas de segurança ou senhas.

Segurança de computadores:
assegure que os sistemas utilizados estejam atualizados e remova programas sem uso ou versões antigas, use somente programas originais e com códigos de licença ativos e pagamento em dia. Faça backup periodicamente, crie um disco de recuperação dos sistemas e impeça a instalação de aplicativos por parte dos usuários.

Conclusão

Além das incontáveis facilidades criadas juntamente com a internet, surgiram também riscos e toda uma gama de possibilidades de fraudes e ataques criminosos. Agora, mais do que nunca, nossos dados pessoais e as informações das empresas valem muito. E é nesse valor que os criminosos digitais estão de olho. Por isso, é preciso adotar uma série de cuidados ao usar a internet para garantir a segurança.

O elemento mais importante para garantir que nenhum problema vai acontecer com seus dados ao usar a internet é o bom senso. Associado à mesma dose de desconfiança que você teria ao receber uma proposta tentadora de um desconhecido na rua, o bom senso é o que vai realmente evitar que você e sua cooperativa venham a cair em golpes na internet.

Como orientação geral, o mais importante é verificar sempre quais são as fontes dos conteúdos e dos sistemas que você está consumindo. É imprescindível optar por fontes confiáveis como primeiro e mais importante passo para evitar golpes online.

Além disso, é preciso prestar atenção nas questões tecnológicas envolvidas no acesso à internet. Dispositivos, computadores e sistemas de boa qualidade são recursos importantes na manutenção da segurança na internet. Ao investir em qualidade você e sua cooperativa ficam menos suscetíveis aos riscos inerentes à navegação.

Acima de tudo, é importante pensar que a internet é a representação virtual do mundo real. Então, tanto quanto num centro urbano, há muitas pessoas trabalhando e com o intuito de fazer da internet uma fonte de informação e trabalho. No entanto, os criminosos também encontram oportunidades na internet e estão dispostos a criar meios de enganar e assustar as pessoas para obter vantagens indevidas.

Por isso, invista na sua segurança para fazer bom uso dos recursos disponíveis e aproveitar as vantagens que a internet oferece.

inova.coop.br

SistemaOCB

sistemaocb

somoscooperativismo.coop.br

Contéudo desenvolvido em parceria com

coonecta
COOPERATIVISMO E INOVAÇÃO

coonecta.me