Segurança na Internet: Um Guia Simplificado

Por que pensar em segurança na rede?

Quais os perigos mais comuns na rede?

Como manter-se seguro na rede?

Conclusão

2022

Por que pensar em segurança na rede?

A segurança online é um tema que tem estado cada vez mais em evidência, fato que se deve ao crescimento expansivo das atividades realizadas na web. Hoje, você não precisa mais se deslocar até o seu banco para conferir o saldo da sua conta, alguns toques na tela do celular já são o suficiente para isso. Da mesma maneira como já não é mais necessário sair de casa para fazer depósitos, transferências e pagamentos. Passou-se também o tempo de "bater pernas" de loja em loja para pesquisar preços e comprar aquele produto tão desejado, tudo isso pode ser feito com alguns cliques e, melhor, no conforto da sua casa. Se pararmos para pensar em todas as possibilidades – e facilidades – que estar conectado nos oferece, este parágrafo iria muito longe. Entretanto, meu objetivo aqui não é citar tudo o que você pode fazer estando conectado, afinal isso você já deve saber – e até fazer. Meu objetivo através desse breve escrito é lhe apresentar a melhor maneira de fazer isso, ou seja, com segurança.

Afinal, os dados levantados sobre a ocorrência e tentativas de fraudes e golpes na internet são alarmantes. De acordo com informações divulgadas pela *Serasa Experian* em 2021, **a cada 8 segundos uma tentativa de fraude é feita no Brasil** – somente no primeiro semestre de 2021 foram 1,9 milhão de ataques. Já as informações divulgadas pela *Konduto* – criadora do relatório Raio-x da Fraude – revelam que **70% das tentativas de golpes pela internet ocorrem pelo celular**, afinal com a grande migração dos usuários do computador para o celular, é comum que os golpistas também sigam esse caminho.

Felizmente, a cada dia que passa surgem também novas soluções e formas de se proteger contra os golpistas e contra as fraudes. É justamente sobre isso que falaremos aqui, sobre como você não precisa ficar longe da internet e deixar de fazer suas tarefas de maneira prática por receio de ser lesado em um desses golpes desde que, é claro, adote boas práticas para manter você, seus dispositivos e seus dados protegidos contra essas ameaças. Por isso, as sessões seguintes terão como objetivo alertar sobre os golpes mais comuns na rede, quais são e como ocorrem, e a como evitar ser uma das vítimas - afinal é importante conhecer os riscos que existem, mas ainda mais importante é saber como se proteger.

Quais os perigos mais comuns da rede?

Golpes com diversos enredos

Seja pelo aplicativo do *WhatsApp*, por e-mail, por rede social ou ainda de maneira mais elaborada por telefone ou carta de acordo com informações coletadas em perfis em redes sociais ou bancos de dados, todos os dias ocorrem tentativas de golpes usando de algum enredo mirabolante. A história pode ser sobre a revisão do valor da aposentadoria por um suposto escritório de advocacia, de um processo referente ao Plano Collor para ressarcimento de valores, uma pessoa próxima que entra em contato pedindo ajuda financeira e até mesmo falsos alertas de sequestros de parentes.

Independente da história contada pelos golpistas ou do meio utilizado para contatar as vítimas, esses golpes sempre possuem algo em comum: todos pedem algo, dinheiro, dados, uma recarga de celular... enfim, algo que possa beneficiá-los de alguma forma.

A melhor maneira de se prevenir contra esse tipo de golpe é, em primeiro lugar, manter a calma e raciocinar bem se você receber esse tipo de contato. Isso porque essas histórias são criadas justo para deixar as pessoas eufóricas, assustadas ou angustiadas impedindo que elas usem a razão e fiquem mais suscetíveis a caírem na armação.

Lembre-se que qualquer instituição séria não irá fazer um simples contato por mensagem de WhatsApp ou enviar um link por e-mail para tratar de assuntos que tenham importância, no máximo elas te responderão por essas plataformas após **você** ter efetuado uma solicitação. E, se tratando dos casos em que os criminosos tentam se passar por conhecidos para tentar uma extorsão, tente fazer contato com a pessoa por outro meio de comunicação afim de confirmar se realmente se tratava dela antes de atender a qualquer pedido.

Roubo de Informações

Para muitos pode parecer algo inofensivo, embora atualmente a privacidade na rede e a proteção dos dados sejam assuntos mais levados à sério. Mas, excluindo os casos de roubo de informações bancá-

rias e de documentos, que obviamente podem provocar prejuízos, qual é o risco de informações de menor relevância serem expostas?

São justamente esses dados expostos que tornam você, ou as pessoas próximas de você, vulneráveis à golpes como os citados anteriormente. Poucas informações podem ser necessárias para uma pessoa má intencionada elaborar uma história mais crível a fim de lhe aplicar um golpe. Um simples exemplo: você tem seu perfil em uma rede social cujo conteúdo é todo marcado como público, ou seja, qualquer um pode em poucos cliques saber onde você mora, onde trabalha, seu número de telefone, sua idade, suas atividades e quem são as pessoas próximas de você. Um golpista pode trabalhar sua história em cima dessas simples informações para tentar ludibriar alguém próximo de você.

Por isso é importante ter um cuidado de com quem você compartilha seus dados e suas informações, por mais irrelevantes que elas possam parecer.

Clonagem de WhatsApp

Um golpe já muito difundido cujo os motivos para os aplicantes tentarem podem ser os mais diversos é a clona –

gem do WhatsApp. Se trata de outra pessoa tentando acessar o aplicativo em outro dispositivo utilizando o seu número de telefone, entretanto para isso a pessoa precisa de uma confirmação de que ela é a proprietária daquele número, o que de fato não é. O que o golpista faz? Entra em contato com você pedindo que você informe o código de verificação que é enviado por SMS ou por chamada e, é claro, que o golpista inventa uma história para justificar tal pedido. A história mais comum é que você precisa passar o código para receber uma atualização do aplicativo, o que obviamente é mentira, pois toda e qualquer atualização é feita pela loja onde você realizou o download do aplicativo no seu aparelho.

Para se prevenir deste golpe é importante que você nunca passe seu código de verificação para ninguém e que, caso ainda não tenha habilitado, utilize a verificação em duas etapas – e isso não somente no WhatsApp, mas em qualquer aplicação que você use na rede, ou seja, em suas redes sociais, e-mail e etc. A verificação em duas etapas é um recurso que em qualquer aplicação pode ser habilitada acessando o menu de configurações, normalmente nas sessões de privacidade, segurança ou login.

E-commerce falso

Esse é um caso muito menos pessoal, no qual o golpista não vai até a vítima, mas acaba trazendo as vítimas até ele de alguma maneira. É um tipo de golpe que, quando ocorre é em massa e faz várias vítimas por vez. Costuma ocorrer mais comumente em épocas mais específicas, como Black Friday, por exemplo.

Existem, basicamente, duas formas mais comuns desse tipo de golpe ocorrer:

- quando a loja falsa é uma cópia de uma loja existente, fazendo com que as vítimas mais desatentas ao procurar por uma loja em específico caiam no e-commerce falso por acidente. Nesse caso é importante conferir se você realmente acessou a loja correta, apenas conferindo o endereço eletrônico já dá para ter uma noção uma vez que cada domínio é único.

- quando a loja falsa até se diz única, tem nome próprio e, em certos casos, até estratégias de marketing. A forma como atingem seu público é com ofertas muito abaixo do mercado e promoções absurdas de produtos que nunca chegam. Um exemplo bem famoso desse tipo de e-commerce falso foi a "*1,2,3 Importados*". Por isso, se você pretende comprar algo online, realize uma pesquisa prévia em algumas lojas diferentes para ter alguma noção

do quanto o produto custa em média para não cair nesse tipo de cilada.

Embora essas falsas lojas normalmente tentem lesar o cliente na venda de um produto inexistente, normalmente tendo como única forma de pagamento disponível o boleto bancário justo para tornar mais difícil para a vítima recorrer quando perceber que caiu em um golpe, algumas podem querer inovar aceitando outras formas de pagamento para roubar seus dados, como informações de cartões de crédito.

Por isso, procure sempre realizar suas comprar em lojas de confiança, que possuam informações contundentes – como uma forma de entrar em contato, caso você necessite, um SAC e certificados de segurança. Se por acaso seu navegador alertar que o endereço não é seguro, não pense duas vezes e saia do endereço.

Uma dica aqui é, caso você não conheça e confie em uma determinada loja, pesquise sobre ela no *Reclame Aqui,* um site que reúne reclamações e experiencias de usuários de lojas e prestadoras de serviços online.

Como manter-se seguro na rede?

Embora saber dos golpes que ocorrem pela internet seja algo interessante para se manter alerta, a melhor maneira de se proteger de ameaças na internet é através da adoção de boas práticas quando o assunto é segurança e privacidade. Tomando apenas alguns cuidados, as chances de cair em algum golpe se tornam muito mais remotas. Vejamos algumas práticas simples, mas que podem fazer toda a diferença quando o assunto é segurança:

1 – Utilize senhas fortes

Pode parecer um assunto batido, mas a verdade é que muita gente ainda subestima o uso de senhas fortes. Entretanto, boas senhas vão muito além de uma única senha longa e complexa que é usada em todas as contas possíveis ou durante muito tempo, vulgo, anos.

Ainda mais com os vazamentos de dados, incluindo senhas,

Ainda mais com os vazamentos de dados, incluindo senhas, que ocorrem de tempos em tempos, é importantíssimo ter senhas que, além de fortes, sejam únicas para cada conta e alteradas com certa frequência.

É claro que, com o tanto de aplicações e sites que pedem o uso de senhas atualmente, administrar todas essas senhas pode realmente ser uma tarefa complicada. Justamente por isso que um ótimo aliado na sua proteção são os **gerenciadores de senha**, onde você ao invés de precisar memorizar uma série de senhas diferentes, precisará apenas de uma senha segura o bastante para usar essa aplicação e o gerenciador fará todo o trabalho de gerar e administrar as senhas para todo o resto.

Outro ponto importante a ser frisado é que, quando se trata de senhas, nunca deixe-as anotadas em lugares dos quais possam ser roubadas facilmente por um invasor, como no bloco de notas da área de trabalho do computador ou na lista de contatos do celular.

2 - Não dispense o uso de um bom antivírus

Malwares e programas danosos estão entre as ameaças cibernéticas mais comuns que podem danificar os computadores. Embora na maioria dos casos causem ape–

nas aborrecimentos, existe sim o risco da ameaça ser mais séria e provocar danos maiores, como o roubo de arquivos e de dados do seu navegador, por exemplo. Um bom antivírus normalmente já é o suficiente para bloquear qualquer malware imediatamente, além disso alguns podem já vir com funcionalidades extras bem úteis como gerenciadores de senhas e ferramentas anti-phishing.

Manter habilitados também as ferramentas de proteção nativas do sistema operacional que você estiver utilizando também é importantíssimo para que não haja furos na sua segurança. Um exemplo dessas proteções nativas do sistema é o **Firewall** que aplica as políticas de segurança à conexão.

3 – Tenha cautela ao utilizar redes públicas

É preciso agir com mais cautela ao utilizar redes públicas, seja uma rede móvel pública de fato onde você vai se conectar com seu smartphone ou com seu computador portátil ou ainda ao utilizar um dispositivo que não é o seu particular.

Em redes públicas há o risco de haver o que é chamado de “man in the middle”, alguém que se aproveita de redes públicas para roubar dados que estão sendo transferidos

naquela rede. Em redes públicas há o risco de haver o que é chamado de *"man in the middle"*, alguém que se aproveita de redes públicas para roubar dados que estão sendo transferidos naquela rede.

Por isso, se você não estiver em uma rede de confiança, geralmente aquela da sua casa, evite acessar sua conta bancária ou qualquer outra coisa de semelhante importância, deixe para fazer aquela compra online ou dar aquela conferida na conta corrente quando estiver na segurança de sua rede particular.

Já ao utilizar computadores públicos, como os de bibliotecas, por exemplo, nunca concorde com a caixa de diálogo que pergunta se você quer que aquele computador ou navegador lembre de você ou salve sua senha. Além disso, faça o *logoff* de todas as sessões que você iniciou antes de se desconectar.

Parece até bobo falar disso, mas muita gente já clicou nessas caixas de diálogo sem querer – fosse por desatenção, pressa ou até inocência. Uma dica é: sempre que usar um navegador em um computador público, opte por utilizar a **guia anônima** que, assim que fechada, "esquecerá" os dados que foram inseridos.

4 – Tenha muito cuidado com o *phishing*

O phishing pode vir em diversas formas e ter diversos objetivos, mas de qualquer maneira ele sempre é malicioso. Basicamente, os golpes citados anteriormente são, em sua maioria, formas de phishing. O fato deles variarem tanto tem a ver com a criatividade e o objetivo dos *phishers*, que podem ser os mais variados. As formas mais comuns são de phishing são:

- E-mails contendo links maliciosos ou anexos que possuem malwares;
- Sites e páginas de login falsificados;
- SMS's com links para acessar alguma página ou baixar algum aplicativo;
- Invasões em redes sociais, fazendo com que as contas das vítimas enviem links maliciosos para seus amigos;
- *Vishing*, que nada mais é que o phishing por voz, ou seja, em forma de chamada. Nesse caso, o golpista tenta convencer a vítima a divulgar informações pessoais ou a pagar algum valor utilizando de alguma história para convencê-lo. Muitas dessas chamadas de vishing são automatizadas e muitas das chamadas de números ale–

atórios que as pessoas recebem diariamente em seus telefones e celulares são tentativas de vishing.

Existem bons antivírus que ajudam na proteção contra o phishing, mas ter atenção aqui também ajuda bastante. Como já dito anteriormente, seu banco, sua operadora de seguro, uma loja com a qual você nunca teve nenhum contato não chegarão em seu *imbox* fazendo ofertas mirabolantes.

As lojas até podem acabar enviando e-mails com links de promoções caso você seja cadastrado para receber essas ofertas ou você tenha começado uma compra e ainda não finalizado, mas se não for o caso ou você ache suspeito, nunca clique nesses links. Prefira acessar o quer que seja sempre da maneira mais segura possível.

5 – Dê preferência para sempre acessar sites seguros

Existe por aí uma quantidade imensa de sites que talvez até não sejam maliciosos, mas que não são seguros. E, como já dito antes, existem aqueles que claramente tem o intuito de roubar dados, danificar os dispositivos com malwares, enfim, lesar a vítima de alguma maneira.
Sempre garanta que a página que você está acessando na web é legítima e segura. Isso pode ser feito observando se

o endereço da página não possui erros de ortografia, se no rodapé da página existem as informações de contato da empresa, se a página possui os selos de segurança e se possui o protocolo https de navegação segura.

Concluindo

Como você deve ter percebido ao longo de sua leitura, não existe uma fórmula mágica ou uma técnica muito complexa que somente *hackers* entenderiam para ficar seguro – ao menos na *surface*, essa camada da rede que usamos diariamente. Pequenos cuidados, um pouco de atenção aqui e ali e colocar em prática coisas que ouvimos volta e meia sobre segurança na internet – como usar um antivírus ou não clicar em qualquer link – são sim capazes de lhe manter seguro, mesmo que pareça pouco ou que pareça simples.

Afinal, aparentemente os golpistas gostam de pessoas desavisadas, desatentas e que se impressionam fácil, isso desde o tempo em que os golpes eram dados pessoalmente. Um usuário que segue boas práticas, que não sai clicando em tudo o que vê e não se ludibria com uma oferta incrível de uma loja online da qual nunca ouviu falar não é exatamente o perfil de quem mais cai em golpes.

Espero sinceramente ter colaborado em algo para você

através desse singelo escrito. Seja na conscientização de que o risco existe, apresentando uma informação a qual lhe era desconhecida ou de fato uma solução para lhe deixar mais seguro ao navegar pela internet. Afinal, na internet existem sim aqueles mal intencionados, fraudes e perigos, entretanto também existe muita informação, entretenimento e, com a evolução dessa tecnologia, nos trouxe uma série de funcionalidades que tornam nosso cotidiano mais prático. Para usufruir do que há de bom basta fazer um bom filtro das coisas e, como já citei inúmeras vezes, adotar boas práticas.

Fique à vontade para voltar a este arquivo sempre que sentir que está com alguma dúvida nos assuntos que aqui foram abordados e sinta-se convidado a descobrir mais sobre o assunto e a adotar ainda outras práticas mais que auxiliem em sua segurança.

Existe muito conteúdo útil e excelentes tutoriais que ensinam a, por exemplo, habilitar a autenticação em duas etapas nos aplicativos de comunicação, extensões para o navegador e aplicativos que rastreiam ofertas e denunciam fraudes em e-commerces, enfim, existe muito conteúdo que lhe ajudará a aprender como manter-se protegido enquanto faz aquilo que gosta na internet.

Quem sou eu?

Jéssica Siedschlag Alves

Estudante do curso de Tecnologia em Análise e Desenvolvimento de Sistemas pela UNINTER (Universidade Internacional de Curitiba). Alguém que, provavelmente como você que está lendo, também preza por sua segurança e privacidade quando o assunto é internet e que, infelizmente, já teve pessoas próximas sofrendo diversas tentativas de golpes aqui na rede e por isso, decidiu abordar esse assunto, mesmo que de forma superficial, a fim de tentar colaborar de alguma maneira para que cada vez menos pessoas sejam vítimas de pessoas mal intencionadas na internet.