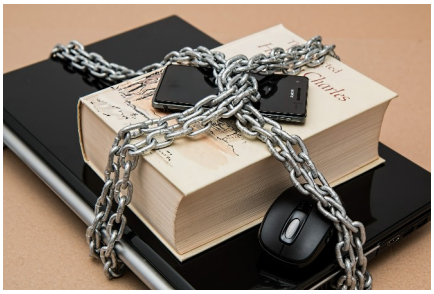
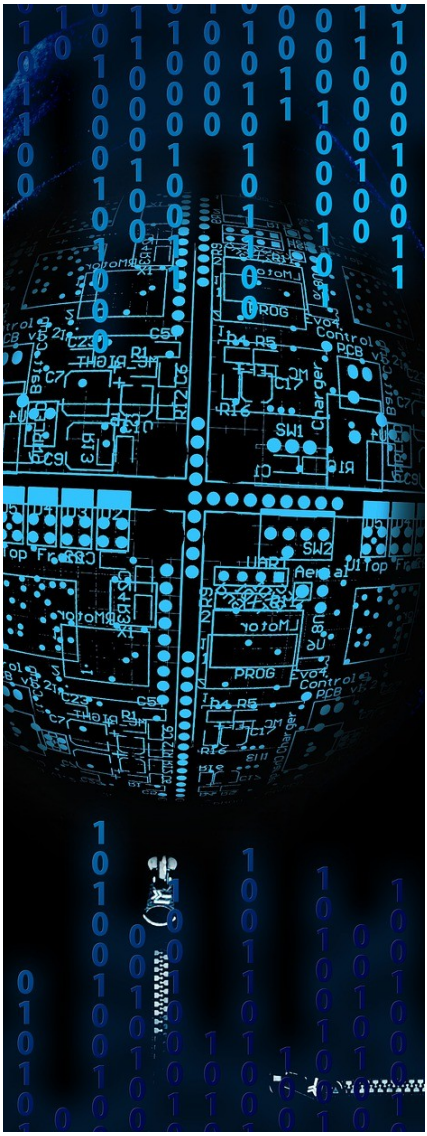
Autoria: Silvio Ferreira
Finalidade: educativa e comunitária (Extensão UniCV)

Essencial saber





No capítulo passado tivemos um importante embasamento sobre vírus, onde podemos constatar os principais tipos de vírus que podem contaminar computadores, desde os pseudos vírus aos mais perigosos worms. Vimos também que os vírus podem ser construídos de forma simples, muita vezes até "bobas" usando técnicas nem um pouco tecnológica mas que se o usuário não estiver preparado, principalmente se o usuário estiver mal informado, poderá perder todos os seus dados. Outros vírus porém são bem mais "modernos" usando técnicas de propagação pela rede

e até pelos e-mails, se replicam, instalam trojans entre outras coisas.

Então de nada adianta dizer: "isso nunca irá acontecer comigo", "o meu computador nunca irá pegar vírus", o "meu computador nunca será invadido", etc.

O que deve ser feito é tomar algumas medidas simples, que na maioria das vezes são eficazes.

Esse capítulo é um complemento ao anterior, mas agora estaremos vendo como se proteger de vírus e hackers, quais os reais riscos, as medidas de segurança elementares que todos podem aplicar. O nosso objetivo aqui é apresentar a todos um modelo simples de segurança que visa:

- Trabalhar com segurança física e lógica;
- Conhecer os principais tipos de vírus e combatê-los com antivírus;
- Preservar a privacidade do usuário e a segurança dos dados usando firewalls e anti-trojans;
- Cultivar atitudes seguras, o que inclui: conscientização do uso correto de senhas, e-mail, identificação de sites seguros e, por fim, identificação de informações idôneas.

O que é segurança?

Segurança possui um significado amplo. Afinal, estamos falando de segurança de quê? E é física ou lógica (segurança da informação)?

Se formos falar sobre segurança lógica, podemos definir (de forma bem elementar) a segurança como a restrição dos recursos de um sistema para um ou um grupo de usuários definidos e a proteção dos dados. Temos a segurança quando haver a gestão de tais restrições, constituindo assim uma política de segurança.

Não adianta usar os melhores softwares e hardwares se haver falhas humanas, se as pessoas não souberem gerenciar tais recursos, o que leva a concluir que segurança é antes de tudo uma questão humana e não técnica. Os elementos que compõem a segurança lógica são:

- **Integridade:** evitar problemas causados por vírus (pois eles podem apagar dados, abrir brechas para um invasor, etc;

- **Confidencialidade:** as informações estão disponíveis somente ao usuário devidamente autorizado;

- **Disponibilidade:** os recursos estão disponíveis sempre que necessário.

Um sistema não está protegido ou há falhas na segurança quando:

1- É contaminado por vírus. São instalados aplicativos não autorizados;

2- Informações são acessadas/lidas/copiadas por pessoas não autorizada, seja remotamente ou não;

3- Informações são alteradas por pessoas não autorizada;

A segurança não se limita somente ao meio lógico, ela é dividida em:

- **Segurança lógica:** segurança de um sistema e de seus dados e, segurança dos usuários do sistema, suas informações/dados pessoais e privacidade.

- **Segurança física:** é a segurança do local propriamente dito, treinamento constante dos funcionários. Se um funcionário encontra um pen drive na calçada da empresa e simplesmente conecta ele no computador da empresa existe uma falha aí, uma falha humana, uma falha de treinamento e falha física (afinal, o pen drive que estava na calçada foi para dentro da empresa).

De nada adianta instalar em um sistema o melhor sistema de segurança, se alguém não autorizada conseguir sentar na frente do computador e obter acesso as informações.

Todos os usuários (ou pelo menos grande partes deles) cuidam, ou deveriam cuidar, da segurança física mínima do computador, muita vezes sem perceber que a faz, por exemplo: com a instalação de nobreaks, evitando colocar o computador em locais onde há risco de queda de objetos sobre o mesmo (debaixo de prateleiras), etc.

Segurança física

Há segurança física quando:

- O acesso ao computador é restringindo (e controlado) a um grupo pessoas;

- É garantida o funcionamento do computador durante um determinado tempo caso ocorra queda de energia elétrica (através de nobreaks);

- É tomada todas as precauções para que problemas na rede elétricos (excesso de tensão, tensão insuficiente ou ruídos), relacionados a fenômenos da natureza (raios) ou curto circuito na rede não interfiram no funcionamento do computador. Isso é feito com filtros de linhas, estabilizadores e nobreaks;

- A instalação do computador é feita em locais apropriados (onde não há risco de queda de objetos sobre ele, onde não há infiltrações de água, etc) em tomadas apropriadas e com uso de aterramento;

- A entrada e saída de dispositivos de armazenamento é controlada.

A segurança física em determinadas empresas é mais importante que a segurança lógica, e o grande exemplo que muitos já está acostumado a ver são em lojas de suprimentos para informática (venda de hardware).

É claro que em casos como esse, a segurança física conta com muito mais recursos, incluindo: serviços de guarda, treinamento adequado dos funcionários, instalação de câmaras, etc.

Esteja sempre atento quanto a segurança física: e você faz isso na instalação de filtros de linha, nobreak, uso de tomadas adequadas (o que evita possíveis curto circuitos), aterramentos, ventilação de ambientes, proteção e eliminação de poeiras, mesas ideais e umidade (entre outros). Tudo isso faz parte da segurança física.

Segurança lógica

A segurança lógica é o que expliquei no início do capítulo. Ela visa a proteção dos dados de um computador para que não sejam apagados ou copiados dados indevidamente, que o sistema esteja sempre acessível quando necessário, etc.

Quais os reais riscos?

Os riscos reais são os vírus que podem chegar através de anexos de e-mails, vírus disfarçados de programas benignos (trojans) baixados pelo próprio usuário em sites desconhecidos, boatos (que induzam o usuário a apagar algum arquivo) e o acesso ao sistema por pessoas não autorizadas (exemplo: hackers).

Mas é preciso esclarecer que os sistemas domésticos (computadores) são de longe, muito mais atacados por vírus do que por hackers.

O que pode levar um hacker a invadir um computador doméstico é quando o usuário instala (sem saber que fez isso) um trojan.

Em outras palavras, o usuário é quem facilitou a entrada do hacker.

Logicamente um hacker pode tentar invadir um computador de outras formas que não seja usando um vírus, o que nesse caso, pode não ser tão simples se o sistema estiver com todas as atualizações e demais segurança.

Dessa forma, os principais riscos que afetam um sistema doméstico são:

- **Vírus:** de todos os tipos. Podem apagar, modificar ou corromper dados. Podem permitir a entrada de um hacker;

- **Boatos:** Apesar de parecer ridículo, pode acontecer do usuário receber uma mensagem com textos do tipo "pior vírus do mundo", pedido para o usuário deletar um arquivo específico o mais rápido possível, pois trata-se de um vírus capaz das piores "malvadezas" que se possa imaginar. Nesse item se encaixa também informações provenientes de sites não confiáveis;

- **Hackers:** Como disse anteriormente, os hackers representam um risco menor do que os vírus aos computadores domésticos. Se os hackers atacassem os computadores na mesma proporção que os vírus, seria o mesmo que dizer que praticamente todos os computadores que acessam internet estão sendo, ou já foi, invadidos por hackers, o que não acontece. Isso porque a quantidade de computadores que tem ou já tiveram problemas com vírus é gigantesca. Ressalto também que nem sempre uma pessoa que obtém acesso (seja remotamente ou não) não autorizado a um computador, será um hacker. Por isso é preciso sempre se prevenir. Se um hacker invadir um computador, ele pode roubar dados sigilos do mesmo, instalar vírus, apagar dados, ou na pior das hipóteses, iniciar um ataque a parti do computador invadido.

Por que se preocupar com segurança?

Para proteger nossas informações confidenciais. Imagine se uma fotografia pessoal, ou uma "carta" (qualquer texto digital, seja e-mails, em programas de comunicação instantânea, etc) escrita para alguém, ou até mesmo um livro como este, seja copiado por uma pessoa não autorizada.

E pior, imagine se essa pessoa coloque o que ele pegou disponível na Internet. Para evitar isso é preciso segurança.

Com certeza você já fez alguma comprar pela internet (ou conhece alguém que fez). Durante essa compra foi digitado o número do CPF, endereço, telefone, e talvez até o número do cartão de crédito.

É preciso haver segurança para que transações desse tipo possam ocorrer sem problemas.

É preciso haver segurança para que pessoas não autorizadas não usem a sua conta de acesso à internet.

É preciso haver segurança para que pessoas não autorizadas não acessem aos seus e-mail.

É preciso segurança para que pessoas não autorizadas não acessem o seu computador PC, tablet, celular, notebook, etc.

A integridade das informações contidas em um sistema depende do quão seguro ele é.

Além disso, um ponto importante a saber: em uma rede doméstica, todos os dispositivos devem estar protegidos. Se apenas um deles estiver desprotegido, o esquema de segurança está deficiente, pois, possui um ponto vulnerável, que pode a partir dele disseminar vírus e comprometer a integridade das informações que circulam pela empresa, etc.

Além disso, como disse, a segurança não se restringe somente aos dados.

A segurança é necessária para que nas lojas não haja furtos e para que os equipamentos que lá estão não sejam danificados.

E tudo isso vale plenamente para qualquer computador pessoal.

Segurança mínima

As regras para manter um mínimo de segurança possível são:

1. Tenha sempre um antivírus atualizado instalado no computador. Não adianta instalar um antivírus e não atualizá-lo com frequência, pois, novos vírus surgem a todo momento. A tabela a seguir contém o endereço eletrônico de alguns antivírus:

Anti-vírus	**Endereço eletrônico**
Kapersky Anti-Vírus	https://www.kaspersky.com.br/
Bit Defender	https://www.bitdefender.com.br/
Norton Anti-Vírus	https://br.norton.com/
Mcafee Visruscan	https://www.mcafee.com/pt-br/index.html
Panda Anti-Vírus	https://www.pandasecurity.com/en/
AVG Anti-Vírus	https://www.avg.com/pt-br/homepage
Avira Free	https://www.avira.com/pt-br
Avast! Home edition	https://www.avast.com/pt-br/

2. Use um Firewall, que é um programa que auxilia na proteção das informações contidas em um PC. Através do firewall é possível bloquear tentativas de instruções (como a tentativa de instalar ou apagar algum arquivo) bem como o tráfego não autorizados no PC. A maioria dos antivírus atuais possuem a função de Firewall.

3. Use um programa para proteção contra trojans, malware, spyware, etc. A maioria dos antivírus atuais possuem algumas funções extras, como prevenir e remover, trojans, malware, spyware, etc.

Veja na imagem a seguir uma tabela com as funções de alguns antivirus.

Fonte: https://www.antivirusguide.com/pt/a-melhor-protecao-contra-malware/

	kaspersky	Bitdefender	McAfee	Norton	panda
Remove Adware	✓	✓	✓	✓	✓
Proteção Ransomware Dedicada	×	✓	×	✓	✓
Anti-Phishing	✓	✓	✓	✓	✓
Anti-Fraude	✓	✓	✓	✓	✓
Modo de Recuperação	×	✓	×	×	✓
Funcionalidades					
VPN	✓	✓	×	✓	✓
Serviço Bancário Electrónico Seguro	✓	✓	×	✓	×
Proteção de Webcam	✓	✓	×	✓	×
Guia para Pais	✓	✓	✓	✓	✓
Analisador de Vulnerabilidade	✓	✓	✓	✓	×
Firewall	✓	✓	✓	✓	✓
Modo Silencioso	✓	✓	✓	✓	×

Fonte:
https://www.antivirusguide.com/pt/a-melhor-protecao-contra-malware/

Além disso é necessário:

- Fazer uso correto de senhas
- Atualizar constantemente os programas e o sistema operacional através das Patches;
- Ficar sempre alerta com os conteúdos que chegam através de e-mails, principalmente nos anexos;
- Cuidado com sites inseguros.

Senhas

Senhas fáceis de deduzir são as principais causas com problemas na segurança.

Devemos evitar a qualquer custo formular senhas tomando como base:

- Datas de nascimento;
- Número da placa do carro;
- Número de um telefone;
- Nome de pessoas, etc.

Tudo isso é o que chamamos de pistas. Então a senha segura é aquela que não deixa nenhuma pista, não importando em que situação está sendo criado a senha:

1. Para acessar E-mails;
2. Para obter acesso ao computador;
3. Para abrir arquivos;
4. Para efetuar algum login, etc;

Como formular senhas seguras

Uma senha para ser segura deve descartar palavras óbvias (pass, abrir, password, senha, etc), em branco ou mesmo nome do login.

Nunca use:

- Datas de nascimento;
- Número de casa ou apartamento;
- Número de telefones
- Nome da esposa ou marido
- Seu próprio nome ou segundo nome;
- Apelido, nome da empresa, nome de objetos ou ferramentas com que você trabalha;
- Sua profissão;
- Números consecutivos (12345), etc.

Além disso a senha não deve:

- Ser muito curta (palavras com menos de seis caracteres);
- Nunca dever ser a mesma para um grupo de usuários (cada usuário deve ter uma senha individual);

- Usuários não devem acessar o PC com a senha do administrador.

A senha segura é aquela formulada seguindo três regras fundamentais:

- Ela é composta por números, letras e símbolos especiais (@ # $ % * +, etc);

- Fácil de digitar, para que não seja necessário olhar para o teclado enquanto digitamos;

- Fácil de lembrar.

Exemplo de senha segura: ompcsscel.

Mas como lembrar uma senha dessas? É simples. A primeira coisa a fazer é criar uma frase que você se lembre facilmente. Pode ser um fato que aconteceu, um sonho, algo que deseja comprar, etc. Em seguida basta usar as iniciais de cada palavra.

Como exemplo da senha anterior, temos a frase:

Os **M**aiores **P**roblemas **C**om **S**enha **S**ão: **C**riar **E** **l**embrar

Observe que usamos as iniciais de todas as palavras, inclusive as letras "O" (os) e "E" para formar a senha ompcsscel. Mas lembre-se que tem que ser uma frase de fácil memorização, algo que será lembrado sem problemas.

Usando a mesma frase podemos chegar a uma nova senha mais segurara, veja:

Os **M**aiores **P**roblemas **C**om **S**enha **S**ão 2: 1- **C**riar **E** 2- **l**embrar

A senha agora ganha números em sua composição, ficando mais segura ainda: ompcss21ce2l.

E para tornar a senha ainda mais segura, você pode desenvolver uma regra particular, tipo: acrescentar o caractere "#" sempre no início de cada senha. Nesse caso a nova senha será: #ompcss21ce2l.

Não se esqueça que a senha deve ser de fácil e rápida digitação. E nunca anote senhas em um pedaço de papel.

Um ponto importante é que as palavras não podem ser muito repetidas, caso contrário podem ser facilmente descobertas através de softwares especiais. Exemplo: aaabccc. Senhas como essas são o equivalente a senha com números consecutivas.

Senha segura = Fácil de lembrar, difícil de deduzir

E é extremamente comum o sistema exigir o uso de letras maiúsculas e minúsculas, além de caracteres especiais. Fique atento a isso.

Sugestões para manter uma senha segura:

- **Cuidado ao digitar:** pessoas podem ver o que você digita;
- **Troque as senhas:** troque as senhas de período em período (a cada dois ou três meses);
- **Uma senha para cada situação:** nunca use a mesma senha em lugares diferentes (para E-mails, documentos, etc). Se uma for descoberta, todas serão;
- **Fornecer senha:** nunca passe a sua senha por telefone ou E-mail para ninguém. A senha é pessoal e intransferível.

Vulnerabilidades

A vulnerabilidade nada mais é que falhas na segurança, que podem ser erros (bugs) que atingem tanto os programas instalados quanto os sistemas operacionais.

Esses bugs podem surgir na criação ou na implementação do programa/ou sistema operacional.

As patches (atualizações) lançadas pelas empresas são feitas para corrigir erros, conforme vão sendo descobertos. O problema desses erros é que são uma porta de entrada para muitos hackers.

Normalmente há três situações que designam vulnerabilidades:

- **Disponibilidade:** esses tipos de erros podem afetar a disponibilidade de um servidor (tirá-lo do "ar"). Isso geralmente é feito (não é a única forma) através da negação de serviço (DdoS - Distributed Denial of Service), que ocorre quando um conjunto de computadores são utilizados para tirar do ar um ou mais computadores conectados à internet. Os computadores não são invadidos, eles apenas ficam fora do ar;

- **Acesso limitado:** é a invasão propriamente dita, ou seja, essa falhas (que podem ser de softwares ou de configurações humanas) permitem que um hacker acesse o sistema. No caso dos erros humanos acontece, por exemplo, quando o administrador se esquece de trocar as senhas padrões do sistema;

- **Execução de códigos arbitrários:** são falhas que permitem que seja executado de um código arbitrário no computador;

Qual o perigo de um sistema vulnerável?

São uma porta de entrada para hackers, que usam programas chamados "scanners" que "varrem" uma rede em busca de vulnerabilidades remotas, ou seja, em busca de computadores vulneráveis ligados na internet naquele momento.

Os scanners não são ferramentas exclusivas de hackers, são usadas também por administradores de sistemas para varrer e encontrar possíveis vulnerabilidade em redes, sistemas operacionais, bancos de dados entre outros.

Hackers que usam esses programas geralmente não tem um objetivo específico (e geralmente são iniciantes), nem querem tentar invadir uma empresa "x" ou o banco "y". Elas apenas vasculham a rede, usando os scanners que fornecem a eles um conjunto de máquinas que estão vulneráveis.

Esses scanners geralmente "varrem" tanto provedores que tenham conexão com fibras óticas ou a backbones rápidos, quanto computadores ligados a rede através de uma faixa de IPs.

Exemplo: endereços entre 64.x.x.1e 64.y.y.254, o que dá 252 máquinas na internet pública. O scanner pode ainda trabalhar com um banco de dados de Ips pré-definidos, onde quanto maior o banco de dados, maior será a probabilidade do objetivo (encontrar sistemas vulneráveis) ser alcançado.

Em vez de procurar por vulnerabilidades remotas, o hacker pode tentar também procurar somente por uma falhas específica (e se nossos computadores não tiverem essa falha, não estarão na lista do hacker), e isso pode acontecer quando por exemplo o hacker tem uma ferramenta que foi feita para explorar uma determinada falha. Aí ele sai a procura de um computador remoto que tenham essa falha para usar a ferramenta.

Qual a solução?

Visite regularmente os websites das empresas de software para obter os patches de segurança e atualizações disponíveis.

Além disso visite os seguintes sites:

- https://www.sei.cmu.edu/about/divisions/cert/index.cfm e
- https://cve.mitre.org/.

Nesses sites você encontrará uma lista com as vulnerabilidades de diversos softwares e sistemas operacionais.

Melhore a segurança

1. **Instale Patches:** instale patches somente de sites oficiais (ou de sites que você já conhece);

2. **Instale Um antivírus e um anti-trojan, anti spyware, etc:** e atualize regularmente;

3. **Instale um firerwall:** prefira sempre as versões completas (pode ser freeware), nunca use demos;

4. **Sempre alerta:** Em uma rede, um alerta de vírus encontrado em um PC, vale para todos ou outros PC, ou seja, todos devem passar por uma "limpeza geral" do sistema, para evitar que um PC recentemente descontaminado, seja contaminado novamente.

Segurança em E-mails

Os e-mails são as maiores porta de entrada dos vírus, dessa forma é preciso tomar muito cuidado com os arquivos anexo e links.

Mesmo que você esteja recebendo um e-mail de alguém conhecido é preciso tomar cuidado. Não que algum amigo seu resolveu te "sabotar", enviando vírus para você. O problema é que esse seu amigo pode nem saber que vírus estão sendo anexados aos e-mails que ele envia.

Por isso é preciso desconfiar de tudo. Comece pela mensagem que vem no corpo do e-mail. Vamos usar como exemplo a mensagem a seguir:

"*Olá, a quanto tempo! Eu me mudei dai para os Estados Unidos, e faz um tempo que perdemos o contato e consegui seu email através de uma amiga sua. Vamos fazer assim, eu vou lhe mandar meu álbum de fotos se você me reconhecer, me retorna o email. Quero ver se você ainda lembra de mim. :)*"

A mensagem que vem no corpo do texto de alguma forma pedirá a você que abra o anexo. E ela é escrita de tal forma que dará a impressão que você já conhece a pessoa.

Se você receber um e-mail desse tipo de alguém que nunca viu falar e a mensagem não é de muita importância, não tenha dúvida e a exclua.

Vale lembrar que a mensagem anterior é apenas uma em várias outras, então o texto sempre variará.

Um cuidado especial é quanto as mensagens em outros idiomas. Se você não sabe ler em inglês, e recebe uma mensagem com um anexo, encare da mesma forma, pois, muitos vírus que se propagam por e-mails, são de origens internacionais.

A extensão do arquivo não importa muito, pois alguns vírus tem dupla extensão, tipo um_nome_qualquer.jpg.exe. Mas o que você vê é somente um_nome_qualquer.jpg, o que pode acabar passando por despercebido.

Por isso é importante configurar o Windows para mostrar todas as extensões dos arquivos (veja isso mais adiante).

No capítulo 02 expliquei também sobre os hoaxes, que são os boatos que se propagam através de e-mails com intenções maldosas.

Sempre verifique a veracidade das informações que circulam na internet. Se uma dada informação diz que a Microsoft descobriu um arquivo maligno no Windows, e este deve ser apagado, verifique antes de fazer qualquer coisa, no site da Microsoft, lógico. E nunca passe a informação para frente, é comum esse e-mail virem com frases do tipo: *POR FAVOR ENVIE ESTA MENSAGEM PARA TODOS OS CONTATOS DE SUA LISTA!!*

Segurança em sites

Há sites que são seguros e há sites que não são seguros. É preciso antes de tudo que o usuário tenha um bom senso. Não é em qualquer site que entrar que ele pode baixar aqueles "programinhas" que tanto procurava.

Da mesma forma não se deve levar a sério informações de qualquer site antes de averiguar a veracidade da informação. Fazer compras pela internet é seguro, desde que você esteja em um site seguro.

Para realizar compras ou qualquer tipo de transação, verifique antes a procedência do site, se realmente são instituições que dizem ser e através de informações de usuários que já compraram no site.

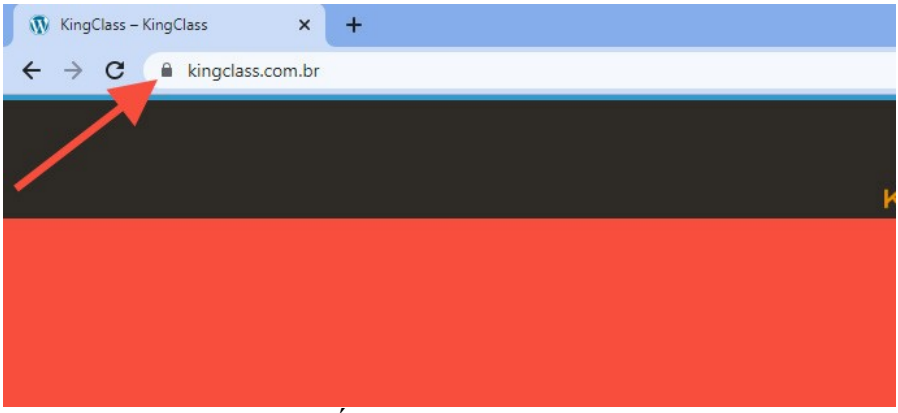
Configura a url do site e o domínio. Você está na URL oficial? Quando você acessa um site com frequência saberá qual a URL dele. Quer um exemplo: qual a URL oficial do Banco do Brasil? É www.bancodobrasil.com.br ou www.bancodobrasil.co? É algo muito simples.

Ao acessar um site, observe se a terminação é .br (exemplo: bancodobrasil.com.br). Se sim, já é algo bom. Mas, isso NÃO significa que sites com outras terminações (.com por exemplo) são ruins, ou são sites que podem ser usados como fonte de ataques. Não estou dizendo isso, em hipótese alguma. Há milhares de sites (ou será milhões?) com diversas terminações (.com por exemplo) que são seguros. O que estou dizendo é que você precisa observar se o site que está acessando possui uma terminação diferente do site oficial, aí sim você precisa ter muito cuidado (e não acessar).

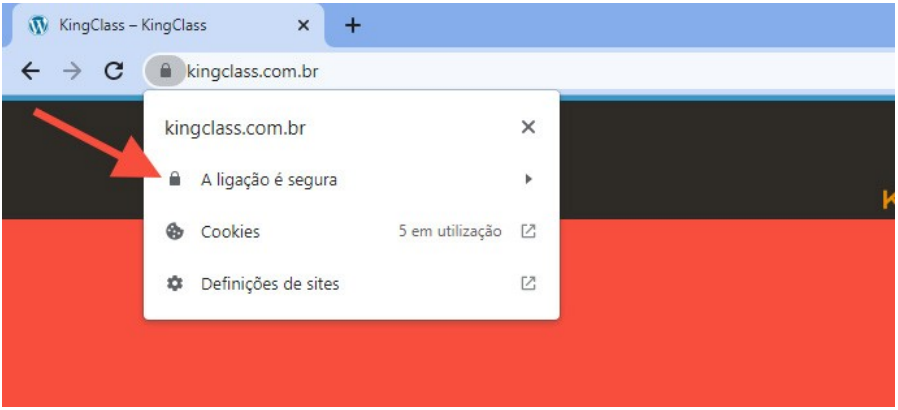
Obviamente pode acontecer de você precisar acessar algum site que você não conhece. Neste caso, verifique se o site possui certificado SSL. Se ele tive, você verá o ícone do cadeado antes da URL.

Ao clicar neste ícone deverá surgir a informação: “A ligação é segura”.

Veja nas imagens a seguir um exemplo.



Ícone do cadeado.



A ligação é segura.

Se o site NÃO tiver o cadeado, significa que nem certificado SSL ele possui. Já é algo a se preocupar.

E você pode usar uma ferramenta do Google para verificar "Estado de site de Navegação segura". Veja esse texto, extraído do próprio Google, que explica a ferramenta:

"A tecnologia de Navegação segura da Google examina milhares de milhões de URLs por dia à procura de Websites inseguros. Todos os dias descobrimos milhares de novos sites inseguros, muitos dos quais são Websites legítimos que foram comprometidos. Quando detetamos sites inseguros, apresentamos avisos na Pesquisa Google e nos navegadores de Internet. Pode pesquisar para saber se é atualmente perigoso visitar um determinado Website."

Endereço eletrônico da ferramenta:

https://transparencyreport.google.com/safe-browsing/search

Em "Verificar o estado do site, digite a URL do site desejado.

A seguir listamos importantes dicas para garantir segurança em sites:

1. Muitos sites são realmente seguros (como os sites de bancos), mas sempre se certifique de estar no endereço eletrônico correto. O endereço pode conter pequenas modificações;

2. Ao comprar qualquer produto, verifique se haverá despesas de envio, prazo de entrega e se há garantia do produto em estoque. Caso haja dúvida em ter ou não o produto em estoque, envie um e-mail (ou ligue pelo telefone) antes para confirmar;

3. Verifique a política adotada pela empresa para a troca ou devoluções de produtos, a garantia;

4. Ao digitar dados pessoais como RG, CPF, entre outros, verifique se você está em uma área segura (representada por um ícone de um cadeado bem na parte inferior do browser);

5. Ao confirmar a compra, sempre guarde todos os dados, inclusive o número do pedido;

6. Sempre certifique se o produto é novo ou usado. Em sites de compra e venda, é comum haver muitos produtos usados. Nesse caso, sempre pergunte (através de e-mails ou outros formas permitidas no site) sobre a conservação do produto. O risco aqui é você fazer uma comprar de um produto "achando" (por engano) que ele é novo, porém, o produto à venda é usado, remanufaturado, produto de vitrine (mostruário), "no estado", "de segunda mão", etc.

Dicas específicas para sites de compra e venda:

- O produto é novo ou usado?

- Qual o estado de conservação do produto?

- Verifique as qualificações (atributos, comentários) do vendedor (se você for comprador) ou do comprador (se você for vendedor). Verifique quantos pontos positivos e negativos ele tem. Verifique a quanto tempo ele é cadastrado no site;

- O produto é original? Em casos de DVDs, verifique se é gravação caseira (feita pelo próprio vendedor);

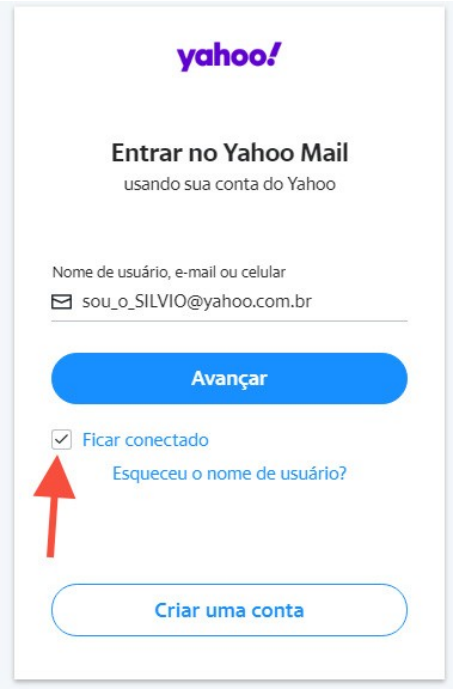
- Por fim, verifique o preço (sempre compare antes, faça uma pesquisa no próprio site), formas de pagamento, prazo de entrega e garantia.

Cuidados com o recurso salvar senha

Em determinadas situações em que digitamos uma senha em um formulário encontraremos uma opção denominada Salvar senha (onde geralmente veremos, a cada vez que formos acessar o sistema, o formulário com a senha preenchida em forma de asteriscos), e Ficar Conectado (onde costuma acessar o sistema automaticamente, pulando o formulário onde deveríamos digitar a senha) ou algo semelhante.

Esse recurso visa facilitar e agilizar o trabalho do usuário, uma vez que ele não precisará digitar a senha novamente, pois, o sistema irá "memorizá-la". E muitas vezes usar esse recurso está mais ligado a preguiça. Sempre que ele for acessar novamente, a senha já estará lá (em forma de asteriscos) ou acessaremos o sistema diretamente, sem o formulário de digitação de senha.

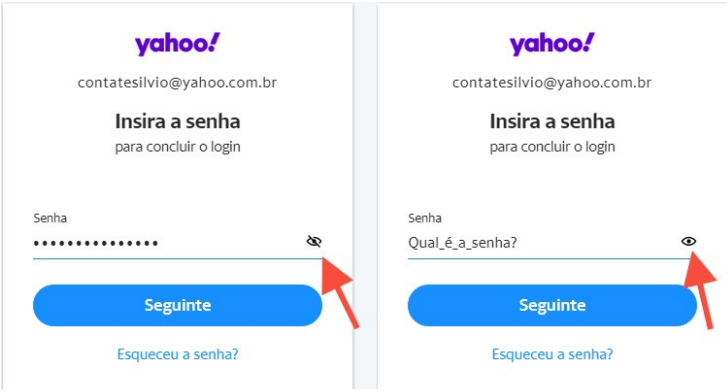
O problema em marcar essa opção é que o acesso ao sistema e/ou a senha estará disponível para qualquer pessoa que tenha acesso ao computador. Se for senha de e-mails, contas em sites, entre outras contas pessoais, qualquer pessoa que acessar esse computador poderá se logar nos respectivos sites e serviços com seus dados.



Veja esse exemplo: opção Ficar conectado

Alguns sites possuem, inclusive, uma opção Mostrar Senha (que pode ser o ícone de um Olho). Basta marcá-la (ou clicar no ícone) e pronto, lá está a senha. Caso o sistema seja do tipo que abre o

formulário preenchido com asteriscos (ele não acessa o sistema pulando essa etapa), qualquer um pode anotá-la.



Veja esse exemplo: opção Mostrar senha.

E mesmo que o site/serviço não possua a opção Mostrar Senha, é possível descobrir o que tem por trás dos asteriscos. Diversas ferramentas desenvolvidas por hackers exploram essas vulnerabilidades.

Inclusive, diversos tipos de vírus conseguem descobrir essas senhas. Já relatei isso para você.

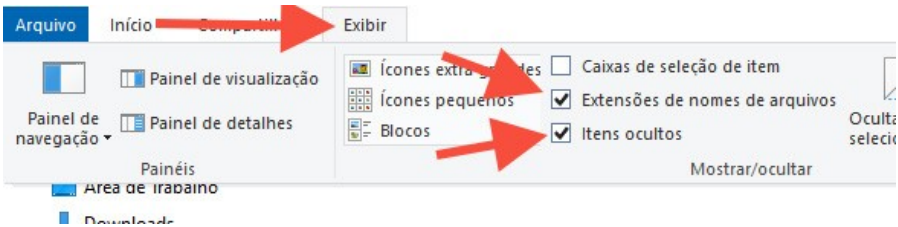
O uso indiscriminado desse recurso coloca em risco a segurança do sistema, pois uma pessoa mal intencionada pode descobrir qual é senha por trás dos asteriscos e qual a senha salva. E isso vale para qualquer computador (PC, notebook, etc) e qualquer outro dispositivo (tablet, celular, etc).

Por defaut, o Windows oculta todas as extensões dos arquivos. O problema é que isso pode se tornar algo inseguro, conforme já expliquei. Um vírus pode se "disfarçar" de uma imagem, tipo jpg por exemplo, poderá ter o nome da seguinte forma: um_nome_qualquer.jpg.exe.

Além disso, o Windows deixa diversos itens de forma oculta. Essa ação é para impedir que o usuário apague acidentalmente arquivos do sistema, é uma configuração de segurança. Mas, por outro lado, arquivos maliciosos também podem usar esse recurso para ficarem bem escondidos.

Para exibir as extensões e arquivos ocultos é simples, veja:

No Windows 10 ou superior, em qualquer pasta que você estiver, clique em Exibir e marque a opção Extensões de Nomes de Arquivos e Itens Ocultos.



Extensões de Nomes de Arquivos e Itens Ocultos