Autoria: Silvio Ferreira

Finalidade: educativa e comunitária (Extensão UniCV)

Essencial saber

Eis que chegamos ao último capítulo deste livro. Foi uma grande jornada até aqui. Estudamos sobre os mais variados tipos de vírus, como agem e o que podem fazer. Tivemos uma abordagem, no ponto, sobre hackers e suas classificações. E não posso deixar de comentar sobre os capítulos que abordaram engenharia social e os principais tipos de golpes que fazem tantas vítimas atualmente. São capítulos importantíssimos. E claro, para fortalecer essa obra, estudamos segurança e os aspectos emocionais que são explorados por hackers, crakers, cybercriminosos no geral e por muitos golpistas.

Para encerrar essa obra com chave de ouro, este último capítulo é sobre segurança.

Segurança novamente?

Afinal, no capítulo 03 já temos uma abordagem bem completa sobre segurança. O que há de ser abordado agora?

Calma. Explico para você em detalhes.

Segurança é um tema extenso. Daria para escrever tranquilamente um livro de 1200 páginas ou mais. Basta pensar um pouco: segurança de qual área? É física ou lógica?

Se for segurança física, envolve segurança local, de transporte, treinamentos de funcionários, dispositivos de segurança (travas, fechaduras, câmeras, etc) e muito mais. Esses exemplos são apenas o básico, é a pontinha do iceberg.

Se for segurança lógica o mesmo ocorre. A segurança da informação é uma tema muito abrangente. Tudo que você pensar existe alguma necessidade de segurança.

Devido a tudo isso, este capítulo foi escrito. Só que há uma diferença aqui: abordei alguns tópicos de tal forma que, juntos, ajudarão a criar a sua mentalidade preventiva.

O que é mentalidade preventiva?

Neste escopo, trata-se de ter mentalidade forjada com práticas de segurança. Algumas situações podem parecer exagero para alguns, mas são fundamentais para outros.

Quer um exemplo de mentalidade preventiva? Simples. Responda as perguntas:

- Você destrói (rasga, picota, queima) todos os extratos bancários antes de jogá-los no lixo?

- Você se certifica em não jogar no lixo nenhum documento/papel que contenha seu nome e CPF? Antes de jogá-los, rasga e picota eles?

Se a resposta foi sim, significa que você já possui mentalidade preventiva.

A mentalidade preventiva é forjada naquilo que fazemos e como fazemos. São nos hábitos simples que temos em cada situação, nas decisões tomadas, na forma com que usamos e usufruímos de recursos, serviços, pessoas e muito mais.

Boas Práticas Gerais de Segurança

- **Descarte de papéis:** um cuidado fundamental, para pessoas físicas e empresas, é quanto ao descarte de documentos e papéis importantes: notais fiscais, contas, extratos, via de pagamento do cartão e tudo mais devem ser destruídos antes de serem jogados no lixo. Picote ou queime.

- **Backup de dados:** isso vale para todos. Já presenciei um caso real de um vizinho que teve sua casa arrombada por ladrões. Levaram de tudo que se possa imagina, e inclusive um notebook. Nesse notebook havia fotos de suas filhas. Como não existia nenhuma backup dessas fotos, todas essas preciosas lembranças foram perdidas para sempre. Fazer

backup (cópias de segurança) de tudo que é importante é uma decisão fundamental. Faça cópias, pelo menos da forma mais simples que é através de um pen drive. E mantenha esse pen drive bem escondido. Mas, não confie somente em um pen drive, ele pode queimar. Uma excelente opção é armazenar em algum drive virtual, como o DropBox, Google Drive, Adrive, Mega e OneDrive. Todos possuem opções de armazenamento gratuito.

- **Vírus:** cuidado com vírus, já tivemos a oportunidade de estudar muito sobre esse assunto. Em dispositivos móveis eles podem chegar em forma de app e roubar informações e dados sigilosos, etc. Em computadores podem roubar informações, apagar arquivos, causar lentidão ou travar o sistema, etc. Alguns sintomas:

    - **Arquivos deletados:** é comum surgir (principalmente quando se inicia o sistema) mensagens do tipo "não foi possível encontrar o arquivo um_nome_qualquer.DLL", ou o sistema nem conseguir iniciar o computador, retornando mensagens que não foi possível encontrar algum arquivo. Outros arquivos podem simplesmente "sumir", como arquivos de textos, tabelas e na pior das hipóteses, a formatação completa do HD/SSD;

    - **Computador travar:** o computador pode travar por vários motivos, e um deles, pode ser vírus;

    - **Lentidão:** ao abrir programas, ao fechar programas, ao conectar na internet, ao iniciar o computador ou até mesmo ao desligar. O motivo pode ser vários, e um deles pode ser vírus;

- **Imprimir caracteres que não foram digitados:** acontece geralmente nos programas do Microsoft Oficce como o Word, provocados por vírus de macro;

- **Mensagens na tela:** surgimento repentino de mensagens que nada tem a ver com algum programa ou erros do sistema operacional. Já estudamos isso neste livro.

Como Usar E-mails Com Segurança

O e-mail é uma ferramenta extremamente importante usada na comunicação entre pessoas, empresas e serviços.

Usar e-mails com segurança simples se você entender que existe um ecosistema digital dentro do seu e-mail. Esse ecosistema digital é formado pelos e-mails que você recebe de forma comum, esperada e tudo dentro da sua normalidade: e-mails de fornecedores, clientes, parceiros comerciais, aplicativos, provedores de serviços de dados terceirizados, etc.

Tudo que estiver fora da normalidade não precisa ter nem 80% da sua atenção.

Eu, Silvio Ferreira, tenho uma regra pessoal: e-mails que estão fora de meu ecosistema não são sequer abertos. Simples assim. Amigos e familiares NÃO me enviam e-mails, pois, eu converso pessoalmente com eles. E quando há a necessidade de algum e-mail por parte deles, são e-mails já esperados, aguardados.

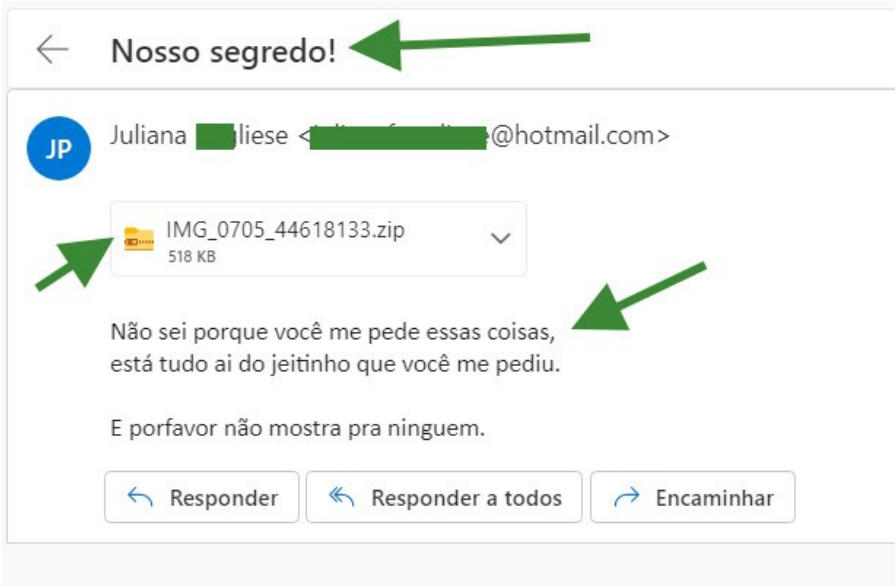
O motivo é muito simples: umas das formas mais simples de contaminação por vírus é através de e-mails (que tem algum anexo

com vírus) “supostamente” enviados por amigos e familiares. Não significa que algum amigo ou familiar seu está enviando vírus para as pessoas propositalmente. Significa, simplesmente, que o sistema do seu amigo ou familiar está contaminado por vírus, e eles nem sabem que mensagens usando os e-mails deles estão sendo disparadas carregando vírus.

Veja bem: e se você receber um e-mail de algum amigo seu dizendo “veja essas fotos, a cara dela ficou hilária”. É correto abrir o anexo? Depende, vamos pensar um pouco:

- Você já tem o hábito de ficar trocando “fotinhas” e demais coisas com seus amigos em e-mails? Se sim, é natural para você. O seu ecosistema digital não é nem um pouco sério e nem seguro. Em uma dessa trocas pode vir, algum dia, vírus.

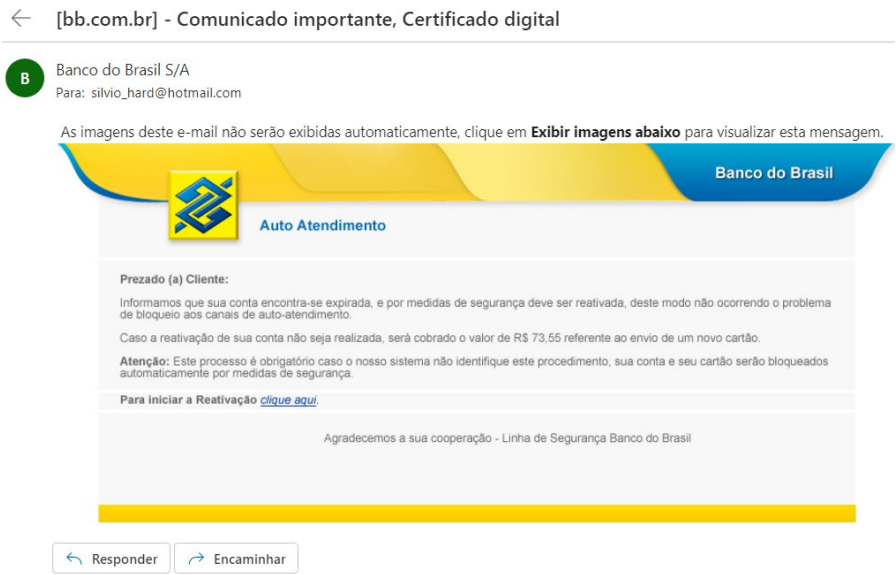
- Ou, isso não é normal para você. Você não faz esse tipo de coisa, seus amigos não fazem isso, o seu ecosistema digital é sério, é para trabalho, estudo, etc. Pois bem, saiba que pode ser vírus. Inclusive, esse exemplo (de fotos) é real, tenho registrado um caso real do uso desse tipo de isca.



Veja esse exemplo, é um caso real.

Tenha cuidado e atenção com:

- **Mensagens supostamente enviadas por bancos:** muitas vezes podem ser mensagens de bancos que você sequer tem conta. Ou recebimento de algum tipo de fatura que não foi autorizada o envio no formato digital, proposta de crédito, aumento de valores de limites, mensagens de bloqueios, certificado digital, etc. Tudo isso pode ser checado na própria central de atendimento do banco. Não clique em links, não abra anexos sem ter certeza. Se você já recebe faturas no e-mail, então já conhece o padrão e saberá identificar qualquer coisa que está anormal;



Veja esse exemplo. Primeiro, o meu certificado NÃO estava atrasado, Segundo, não uso o cartão mencionado. Terceiro, mesmo se usasse cartão, ao valor que seria cobrado está errado. Quarto, o link que está no e-mail NÃO é do Banco do Brasil. Te ensino como ver para onde o link aponta no próximo item.

- **Link com destino duvidoso:** o ideal é NÃO abrir os e-mails. Há alguns registros de códigos inseridos em e-mails que podem iniciar o download automático de vírus. Mas, se caso já tenha aberto o e-mail, há uma forma simples de verificar (no computador) para onde o link aponta (o destino dele). Usei como exemplo o caso anterior (imagem anterior). Para ver o destino do link, apenas posicione o cursor do mouse sobre o link. Mas, NÃO clique. Agora, observe na parte inferior do seu navegador, bem à esquerda: o próprio

navegador mostra o destino do link em questão. Se o endereço, a URL, que aparece ali NÃO for o original e já conhecido por você, não clique. Com certeza é vírus;

Veja esse exemplo: a URL que o link direciona é diferente, não é do Banco do Brasil. Portanto, é vírus.

- **Propostas absurdas:** de algum tipo de ganho de dinheiro ou qualquer outras propostas. Esses tipos de mensagens são as mais variadas o possível, fique atento. Veja abaixo o "incrível" e-mail de alguém que diz se chamar Sra. Theresa Gross, uma suposta cidadã britânica. Segundo o e-mail, 0 marido morreu recentemente com Coronavírus e ela está atualmente no hospital sofrendo de câncer. Segundo o e-mail, ela quer doar 15.200.000,00 GBP (libras esterlinas) para que você estabeleça uma Fundação para o cuidado de animais em seu país. Fiz uma conversão básica desse valor para real, e deu R$ 96.145.586,08. É necessário comentar alguma coisa?!?


Olá

Theresa Gross <sara[redacted]@gmail.com>

Sex, 21/05/2021 07:19

--
Olá
Meu nome é Sra. Theresa Gross e sou uma cidadã britânica. Meu marido morreu recentemente com Coronavírus e eu estou atualmente no hospital sofrendo de doença do câncer. Meu marido tem um depósito de 15.200.000 libras esterlinas em um banco de primeira linha aqui em Londres. Antes de meu marido ser levado para o centro de isolamento, onde morreu, ele me disse para usar os fundos para estabelecer clínicas de tratamento de animais. Temos um amor especial pelos animais. Devido ao meu estado de saúde atual, não poderei lidar com este projeto. Portanto, quero doar 15.200.000,00 GBP para que você estabeleça uma Fundação para o cuidado de animais em seu país. Uma clínica onde os animais serão tratados gratuitamente em seu país. Vejo na televisão que as pessoas doam fundos para orfanatos e não se importam com os animais. Eu e meu marido queremos fazer a diferença no mundo para que as pessoas entendam que os animais são importantes para a natureza. Informe-me sobre seu interesse para que eu solicite ao meu advogado que prepare um acordo de contrato em seu nome. Não se esqueça que meu estado de saúde é ruim, portanto, quero que você responda a esta mensagem o mais rápido possível para que receba o dinheiro antes que algo aconteça comigo. Estou esperando ouvir de você.
por favor contacte-me com este email [redacted]@gmail.com
Obrigada,
Sra. Theresa Gross

Responder | Responder a todos | Encaminhar

A legenda é por sua conta.

- **Qualquer e-mail suspeito:** tenha cuidado e atenção com qualquer e-mail que não faz parte do seu ecosistema digital, que estão fora do padrão comum, que não seja de seu interesse. Caixa de entrada de e-mails não é vitrine de loja, ou seja, você não precisa ficar dando uma "olhadinha" em tudo que está nela. Se um e-mail é suspeito e não é importante para você, apague-o. Se for muito suspeito, de forma evidente que é vírus/golpe, nem é necessário abrir. É direto para a lixeira.

Como Usar Sites Com Segurança

Você não pode acessar qualquer site e clicar em qualquer anúncio que vê na internet. Se você tiver bom senso poderá navegar tranquilamente na web, usar redes sociais sem problema, fazer compras online, usar aplicativos de comunicação e por aí vai.

O risco está em pessoas que acessam qualquer site e clicam em tudo que vê. Muitas iscas digitais podem aparecer em forma de anúncios, conforme você já aprendeu no capítulo 05.

O primeiro ponto a entender é: o que seria um site seguro? É um site que possui domínio “.com.br”? Sites somente “.com” são inseguros?

Entenda isso definitivamente: em um primeiro momento, a categoria do domínio, a sua terminação (aquelas letrinhas: “.com”, “.com.br”, “app.br”), não é usada para definir se um website é seguro ou não. Essa categoria/terminação é chamada por sufixo.

Existem vários sufixos. Cada sufixo de domínio visa definir o tipo de site representado e onde o site (qual país) ele foi registrado.

Por exemplo: para sites registrados no Brasil exitem diversos sufixos: genéricos, sufixos por cidades, sufixo para universidade, para pessoas físicas, para profissionais liberais e para pessoas jurídicas.

Todos os sufixos de sites registrados no Brasil possuem a terminação “.br”.

Cada país tem um sufixo exclusivo que o representa (e que é registrado dentro do país em questão). Exemplos: sites chineses podem usar o sufixo ".cn", sites australianos podem usar o sufixo ".au" e sites alemão podem usar o sufixo ".de".

Veja esse exemplo: a página inicial em alemão do Google é "www.google.de".

Quem controla os registros de domínios no Brasil é a registro.br e a nível internacional é a ICANN.

Veja alguns exemplos de sufixos de origem internacional:

Sufixos	**Significado**
COM	Atividades comerciais
EDU	Instituições educacionais (escolas e universidades).
GOV	Entidade do governo .
INT	Instituições internacionais, como a OTAN.
MIL	Instalações militares.
NET	Companhias ou organizações que administram grandes redes.
ORG	Organizações sem fins lucrativos e outras que não se enquadram em nenhum dos outros casos, como as ONGs.

Veja alguns exemplos de sufixos de origem nacional:

Sufixos	**Significado**
COM.BR	Atividades comerciais
EDU.BR	Instituições educacionais (escolas e universidades).
GOV.BR	Entidade do governo.
MIL.BR	Forças Armadas Brasileiras
NET.BR	Atividades comerciais
ORG.BR	Atividades não governamentais individuais ou associativas

Apesar do significado dos domínios, saiba que muitos deles são genéricos, ou seja, qualquer pessoa pode registrar. Por exemplo:

Domínios ".com", ".net", ".com.br" e ".net.br" são genéricos. Isso significa que qualquer pessoa pode registrar e desenvolver o seu site. Um indivíduo pode registrar um domínio ".com" e/ou ".com.br" mesmo sem fins comerciais. E pode registrar um ".net" sem ter nenhuma ligação com rede, ele pode montar uma loja virtual, por exemplo, de venda de livros.

Veja a lista de domínios genéricos registrados no www.registro.br":

GENÉRICOS (Para pessoas físicas ou jurídicas)

- APP.BR: Aplicativos;
- ART.BR: Artes: música, pintura, folclore;
- COM.BR: Atividades comerciais;
- DEV.BR: Desenvolvedores e Plataformas de Desenvolvimento;
- ECO.BR: Atividades com foco eco-ambiental;
- EMP.BR: Pequenas e micro-empresas;
- LOG.BR: Transportes e Logística;
- NET.BR: Atividades comerciais;
- ONG.BR: Atividades não governamentais individuais ou associativas;
- SEG.BR: Segurança;
- TEC.BR: Tecnologia.

E há sufixos para cidades, universidades, pessoas físicas, profissionais liberais, pessoas jurídicas, com restrição e DNSSEC OBRIGATÓRIO. Para ver a lista completa, use a URL:

https://registro.br/dominio/categorias/

Mas, qual o perigo? Em que um sufixo pode me ajudar?

O sufixo pode dar pista se um site pode ser malicioso ou não. O maior exemplo é quando você se depara com um e-mail de algum "Banco" (só para citar como exemplo), mas, cujo sufixo do site é diferente do original, às vezes é um sufixo de um outro país (não é do Brasil).

Por exemplo: o site do Banco do Brasil é: www.bb.com.br. Você acessaria se o domínio estiver diferente, como www.bb.net???? Afinal, o sufixo é totalmente diferente do que já conhecemos. E SE, esse terminado com ".net" for malicioso?

Portanto, podemos usar a observação do domínio nesse sentido, em situações semelhantes a essa. Se o sufixo do domínio for suspeito, for diferente do original que você já conhece, então não acesse. Simples assim.

Vou reforçar: isso **não** significa que todos os domínios ".com", ".net", ".gov", ".ninja", entre outros, são inseguros. Não é isso que expliquei aqui. Se você entendeu dessa forma, peço que releia tudo novamente.

Certificados SSL

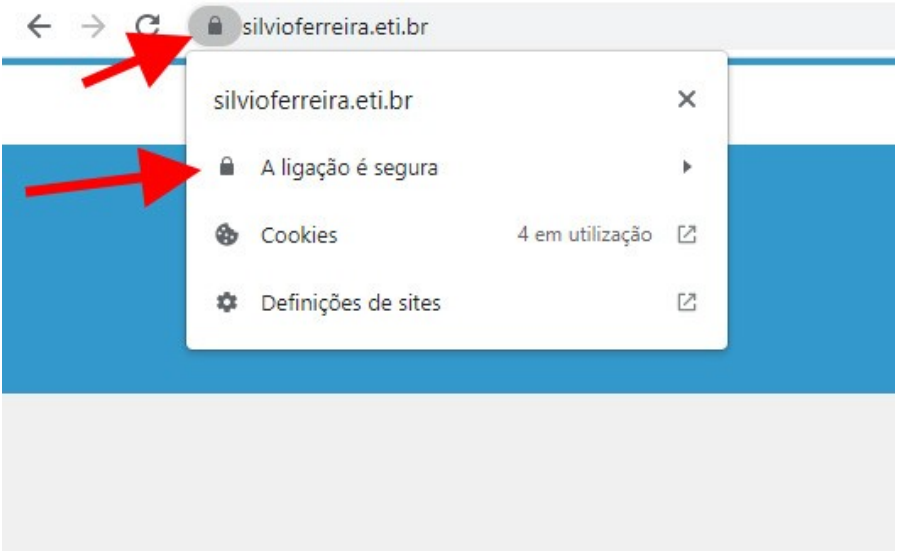
O certificado SSL é um importante indicador de segurança. SSL significa Secure Sockets Layer, que em português é camada de soquete seguro.

Ele é um certificado digital que serve para autenticar a identidade de um website, além de possibilitar uma conexão criptografada. Ou

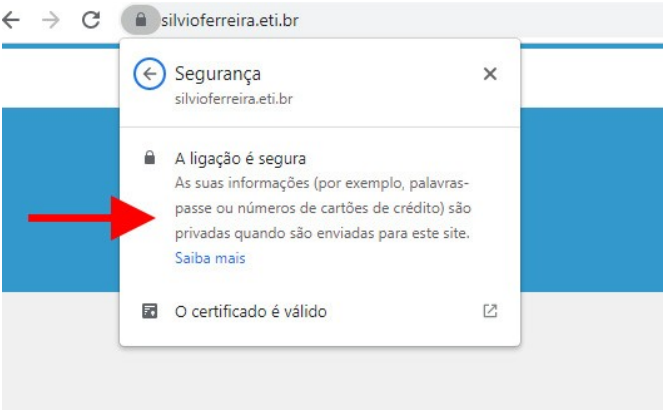
seja, o SSL é cria um link criptografado entre um servidor web e o navegador do usuário.

É graças ao certificado SSL que transações online ficam protegidas. E a privacidade e as informações dos clientes são mantidas seguras.

Como saber se um site usa certificado SSL? Quando um site usa o certificado, você verá o ícone do certificado à esquerda da URL. E se você clicar nele abrirá a informação “A Ligação é segura”.



Veja esse exemplo.



Clique em "A informação é segura" e mais informações serão exibidas.

Vou usar como base o Navegador Google Chrome. São três as possibilidades de ícones/informações:

- **Seguro:** possui certificado SSL. As informações que você envia ou recebe são criptografadas e particulares;

- **Informações ou Não seguro:** o site não possui certificado. Alguém pode conseguir ver ou mudar as informações que você enviar ou receber desse site;

  Não seguro ou Perigoso: o aconselhável é não usar esse site. Ele pode estar enquadrado em uma dessas possibilidades:

- **Não seguro:** muito cuidado. Alguém pode conseguir ver ou mudar as informações que você enviar ou receber desse site;

- **Perigoso:** muito cuidado, não use esse site. A tecnologia de navegação segura do Google já sinalizou ele como Não seguro. Suas informações particulares podem estar em risco.

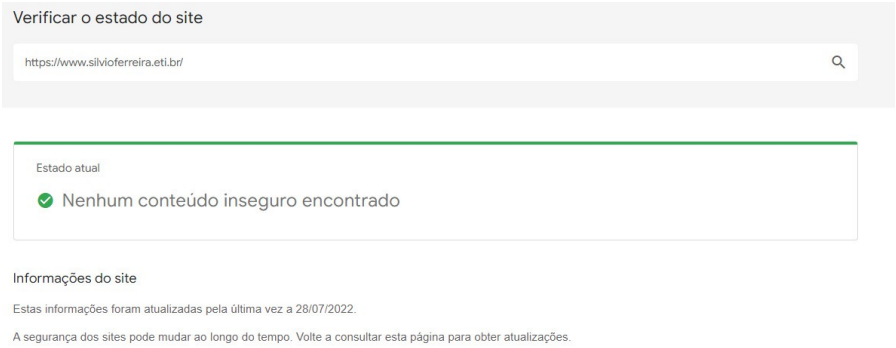
Tecnologia de Navegação segura da Google

Você pode verificar se um website é seguro ou não usando a própria tecnologia de Navegação segura da empresa Google.

"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 detectamos sites inseguros, apresentamos avisos na Pesquisa Google e nos navegadores de Internet. Pode pesquisar para saber se é atualmente perigoso visitar um determinado Website." Fonte: Google.

Para fazer a verificação, acesse a URL:
https://transparencyreport.google.com/safe-browsing/search

Digite a URL completa do site em Verificar o estado do site e dê clique no ícone da lupa.



Tecnologia de Navegação segura da Google.

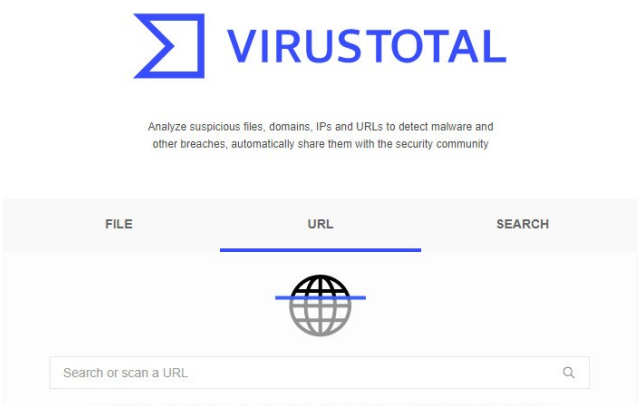
Detectar malware e outras violações online

Existe um serviço online que verifica possíveis ameaças em websites, é o Vírus Total. Bastas digitar a URL e ele vasculha a estrutura de links do site em busca de ameaças.

Basta acessar a URL:

https://www.virustotal.com/gui/home/url

"Analise arquivos, domínios, IPs e URLs suspeitos para detectar malware e outras violações, compartilhe-os automaticamente com a comunidade de segurança". Fonte: Vírus Total.



Vírus Total.

Ferramentas de Segurança do navegador

Todo navegador possui ferramentas de segurança que podem possibilitar Bloquear pop-ups, impedir downloads maliciosos, evitar que você seja rastreado, desativar conteúdos em Flash e até controlar quais sites podem acessar a webcam e o microfone do seu computador e a câmera/microfone do celular.

Verifique esses ajustes de segurança em seu navegador:

- **Chrome:** Configurações > Avançado > Privacidade e segurança;
- **Firefox:** Opções > Privacidade e segurança;
- **Edge:** Configurações > Configurações avançadas;
- **Safari:** Preferências > Privacidade.

Selos de Segurança são confiáveis?

Um selo de segurança não é um indicador confiável de que o site realmente é seguro e livre de vírus e quaisquer outras ameaças. Isso porque, na prática, qualquer pessoa pode copiar imagens de selos e inserir em seus sites. Não confie cegamente em "selos de segurança".

A dica aqui é verificar o site como um todo. Vou deixar um exemplo: se o site não possui certificado SSL, mas, possui imagens de "selos de segurança", tem como confiar? Há uma divergência aqui.

Vale destacar que existem sim, empresas sérias que fornecem selos de segurança para websites que cumprirem com requisitos básicos. Um exemplo é o selo **RA1000** fornecido pelo site www.reclameaqui.com.br. Este selo destaca empresas que demonstram o compromisso com o atendimento ao cliente. Não é todos os sites que conseguirão esse selo. Mas, qualquer site consegue copiar a imagem do selo na própria internet e inserir ele indevidamente em suas páginas. Fica aqui o alerta.

Entre as empresas que fornecem selos, cito:

- **Reclame Aqui:** como mencionei, fornece o selo RA1000. Ele destaca as empresas que possuem excelentes índices de atendimento no site Reclame Aqui. Informações: https://www.reclameaqui.com.br/como-funciona/selo/

- **Norton Secured:** bem conhecido no mercado digital. Passa mais confiança ao cliente devido á marca Norton. Informações: https://www.websecurity.digicert.com/install-norton-seal

- **Site Blindado:** faz análise completa do site, procura por falhas, gera relatório e fornece selo. Informações: https://www.siteblindado.com/

- **E-bit:** selo bem conhecido e respeitado em lojas virtuais. É gartuito e considera as avaliações dos consumidores. Informações: https://www.ebit.com.br/

- **ClearSale:** é uma tecnologia antifraude. Ajuda a atender às expectativas dos clientes com transações mais seguras. Informações: https://br.clear.sale/

- **SiteLock:** possui um conjunto de ferramentas para detectar e corrigir falhas, detectar e eliminar malware, corrigir vulnerabilidades, etc. Os selos/certificados servem para informar aos visitantes que eles estão em um ambiente seguro. Informações: https://www.sitelock.com/

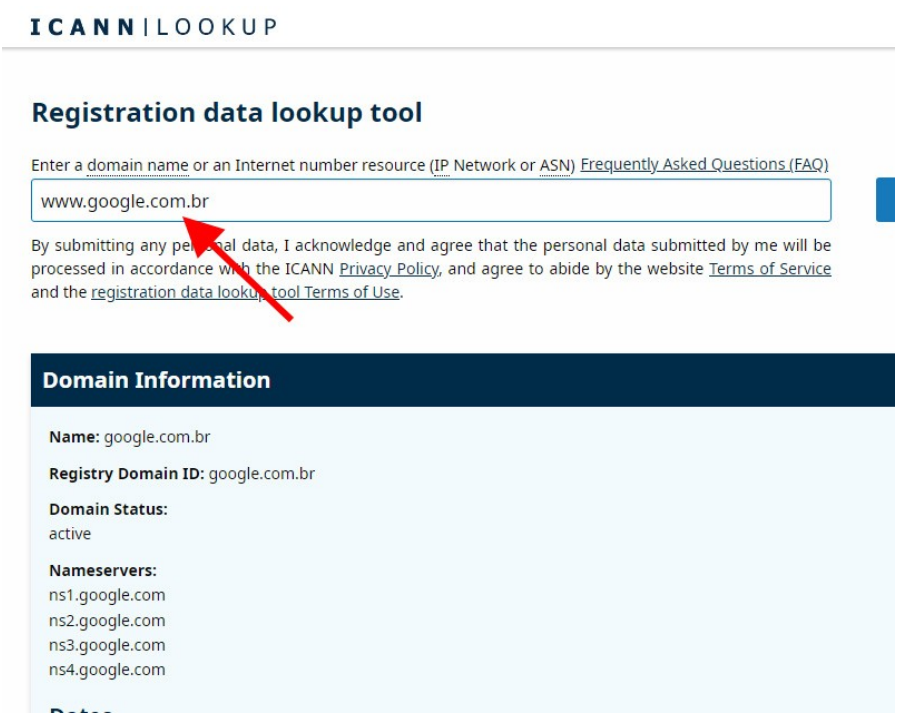
Use o "whois"

caso seja necessário, você pode buscar maiores informações sobre o registro do domínio em questão. Tem como descobrir o nome do proprietário, e-mail, servidores DNS, data de registro, entre outrs informações.

Para isso, acesse o site:

https://lookup.icann.org/en

E em "Registration data lookup tool", digite www, seguido do nome do dominio e dos sufixos.



Exemplo de pesquisa.

Esses sites e serviços SÃO inseguros

E existem alguns tipos de sites e serviços que são inseguros de "nascença". Você pode até utilizá-los, mas estará com o computador sempre "encharcado" de vírus de todos os tipos e de tempo em tempo terá que fazer formatações completa porque até os antivírus não resolverão o seu caso de forma 100% segura devido ao altíssimo grau de risco, aos crackers que tem no seu sistema, etc. E poderá ter problemas mesmo se usar celular, pois, em um algum momento nessas "aventuras" de quem navega nesses sites poderá ser instalado um app malicioso no seu aparelho. São eles:

- **Sites de pirataria no geral:** os famosos sites para baixar programas crackeados, filmes completos e tudo mais. O próprio crackeador que é instalado no programa para que ele funcione já é um risco altíssimo. No mínimo, um monte de anúncios vai começar a aparecer no seu computador.

- **Web sites de conteúdo adulto:** web sites pornôs é o self service de vírus. Existem sites que são confiáveis? Sim. Mas são a minoria. A grande parte vai sim, encher o seu computador de vírus, e app maliciosos no celular;

- **Programas p2p:** aqui é o alto grau, são os "faixa preta". É o nível mais alto. Quer que seu computador tenha vírus e programas maliciosos de todos os tipos? Então junte-se a essa rede. P2P significa peer-to-peer, que em português é ponto a ponto. É uma rede de computadores que compartilham arquivos pela internet. Só que há um porém, não existe um servidor principal para armazenar os arquivos. Ao invés disso, são os próprios usuários que, ao mesmo tempo que fazem download, disponibilizam os arquivos para que outros busquem esses arquivos em sua máquina e façam o download. Tudo sem nenhum tipo de controle ou segurança. E é óbvio que cybercriminosos se aproveitam dessa rede.

Usar Redes Sociais e App de comunicação com segurança

- **Cuidado com mensagens e links recebidos:** já expliquei isso anteriormente. Há muitas formas de você perder o acesso à sua conta;

- **Ative a autenticação de dois fatores:** sempre que tiver essa opção, use-a. É uma forma de segurança à mais e bem mais efetiva. Qualquer tentativa de invasão, troca de e-mail e senha na conta ou até mesmo tentativas de acesso suspeita, irão exigir senhas/chaves de segurança que somente você terá no seu celular. E obviamente, NUNCA forneça essas chaves para ninguém;

- **Não forneça dados pessoais:** nunca forneça dados pessoais para ninguém. Mesmo se for uma pessoa conhecida, pois, pode ser alguém fingindo ser a pessoa que você conhece. Pode ser alguém fingindo ser um parente ou amigo seu. Se alguém pedir algum dado pessoal, ligue imediatamente para essa pessoa, para o número de telefone pessoal dela. Nessa situação, não use o recurso "Fazer chamada" do próprio app, pois, se fizer isso você ligará (fará a chamada) para a mesma pessoa que acabou de enviar a mensagem. Ao invés disso, feche o app, vá na sua agenda telefônica e ligue para o número da pessoa e certifique-se que é ela mesma que te pediu os dados.

- **Não faça pix, não pague boletos, não faça transferência, etc:** o mesmo vale se alguém te pedir um pix (ou pagamento de boleto, transferência, etc), mesmo que diga que é uma situação urgente. Primeiro ligue para a pessoa e certifique-se que é ela mesma que te pediu.

Boas Práticas de Segurança na Internet Para Empresas

- **Treine seus funcionários/Equipe:** realize treinamentos com seu time na área de segurança, boas práticas, etc. Esse livro que você está lendo é uma excelente ferramenta;

- **Controle de acesso à internet:** você precisa ter na empresa um controle de acesso à internet através de senha. Somente pessoas autorizadas é que podem acessar;

- **Não use softwares piratas/crackeados:** o risco de vírus é certo;

- **Programas P2P proibido:** peça ao administrador da rede para bloquear o uso de programas P2P na rede da empresa e em qualquer computador/dispositivo que se conecte á internet da empresa;

- **Regras e política:** defina um politica de uso correto da rede e da internet da empresa;

- **Senhas seguras:** conforme já ensinei neste livro;

- **Sistemas atualizados:** mantenha o sistema sempre em dia com as mais recentes atualizações;

- **Antivirus e Firewall:** instale antivírus e firewall;

- **Backup:** tenha backups sempre atualizados e seguros.

O funcionário da sua empresa é o elo mais fraco?

Já apresentei neste livro, detalhadamente, que a maior vulnerabilidade de todas é o ser humano. Você já sabe porque, os motivos e cuidados que se deve ter. No capítulo 01 já abordei isso:

"Cibercriminosos exploram falhas em sistemas da computação. Usam vírus e diversas outras estratégias para invadir sistemas e roubar informações. Usam dados alheios indevidamente. Geram prejuízos financeiros.

Tudo isso só é possível porque eles exploram, antes de qualquer coisa, a maior falha de todas: a falha humana. Cibercriminosos usam, exploram e abusam de nossas próprias vulnerabilidades. As nossas fraquezas, medos e ambições.

Em todos esses anos de estudo cheguei a uma constatação: muitos cibercriminosos são "profissionais" que estudam, se aperfeiçoam e se dedicam. Não é só programação, é muito além. Eles estudam comportamento humano, psicologia, marketing e muito mais que você possa imaginar."

Entenda isso: se o seu funcionário for mal treinado, não ter nenhuma consciência de prevenção, ele é o elo mais fraco da empresa.

Por isso a importância do treinamento e conscientização constante.

As Fragilidades da sua empresa

- Falta de treinamento de funcionários;
- Não há controle de acesso à internet. Existe até o famoso Wi-Fi grátis para todos que quiserem;
- Funcionários usam softwares crackeados;
- Funcionários usam programas P2P;
- Não há regras e politicas;
- Uso de senhas fracas e senha padrão para tudo;
- Sistemas desatualizados;
- Não há antivírus e firewall, ou estão desatualizados;
- Não existe backup dos dados da empresa.