V1

Aliados Na Sua Segurança Digital

Curso Engenharia da Computação - Uniara

Conteúdo

Capítulo 1

A web, em resumo

Está seção brevemente explica como um site chega no seu computador, pois assim será mais fácil entender o que não se encaixa.

O "protocolo de transferência de hipertexto seguro" (HTTPS[1]) é um processo pelo qual seu computador pede uma página (website) a outro, ele é parte do Protocolo Internet.

Ao ligar qualquer tipo de computador a um roteador, seja por fio ou Wi-Fi, uma das primeiras coisas que acontecerá no Protocolo Internet (IP[2]) é que a fornecedora de internet dará ao computador um número que vai o identificar. Esse número pode se parecer com `52.91.249.136` ou `2804:18:18b8:bcdc:1:0:7fa8:e10`. Isso é como o CEP do computador.

Esses números não são fáceis para humanos lerem. O sistema DNS[3] foi criado para que seja possível ir a um site ou outro serviço usando só palavras ou nomes usando o padrão URL. O URL é como o endereço do computador.

Um URL é assim:

`https://produtos.meusite.shop/amostra`

protocolo://subdomínio.domínio.tld/arquivo

TLD[4] significa um domínio de topo, a parte sempre no final de um endereço. Só é possível registrar um TLD com uma proposta formal a autoridades da internet,

[1] *"HyperText Transfer Protocol Secure"*
[2] *"Internet Protocol"*
[3] *"Domain Name System", Sistema de Nome de Domínio*
[4] *"Top Level Domain"*

então só existem nestes casos:

- Países como Brasil (`.br`), Grã Bretanha (`.gb`) e Itália (`.it`);
- Empresas com grande presença na internet como Google (`.google`), Bradesco (`.bradesco`) e Apple (`.apple`);
- Palavras, para uso irrestrito, como `.com`, `.online`, .chat e `.delivery`.

Qualquer um pode registrar um domínio sob a maioria dos TLDs (exceto os de empresas), mas ainda assim é um processo pago. Por exemplo, o governo cobra R$40/ano por cada domínio `.br`.

Uma vez donos de um domínio, é possível usar qualquer subdomínio que quiser, como `www.` ou `blog.`.

Capítulo 2

Quem é dono deste site?

Agora sabendo como funciona o endereço de um site, é mais fácil perceber quando alguém quer te confundir. Tente responder interpretar os endereços nesses exemplos.

Exemplo 1

`google.eudjgnlw.net`

Lembre-se: qualquer um pode registrar qualquer subdomínio. O site que você está visitando é parte de `eudjgnlw.net`, não Google.

Falso!

Exemplo 2

`havan.gripe`

É de se esperar que Havan tenha o site `havan.com.br` e dificilmente pagaria por mais domínios, seja abaixo de `.gripe` ou de `.shop`. Nesses casos, não acredite no conteúdo a não ser quando dentro do site oficial.

Suspeito!

Exemplo 3

`coca-cola.mcdonalds.com`

Este site não é da Coca-Cola, mas nitidamente é do McDonald's.
Real, mas atenção.

Exemplo 4

`bancocentralbrasil.net`

Se não houver `.gov.br` no final, não é do governo.
Falso!

Exemplo 5

`pagamentosseguro.com.br/vakinha`

O site visitado não é Vakinha. Apenas uma página dentro de `pagamentosseguro.com.br`.
Falso!

Exemplo 6

`mercodalivru.com.br`

Mesmo que pareça Mercado Livre, se uma letra estiver errada, não é.
Falso!

Exemplo 7

`play.globo`

A Globo é uma das poucas empresas com TLD próprio (.globo).
Real, mas uma exceção.

Capítulo 3

Quebrando roteiros de enganação

3.1 Seja inusitado.

Uma boa forma de saber que um site é falso é clicando em tudo menos no óbvio. Um golpista normalmente só foca na parte que tira seu dinheiro, então é importante fazer as perguntas erradas.

Caso você tenha em sua frente "clique AQUI para comprar geladeira" numa loja de departamentos, pare e digite "aspirador de pó" na barra de pesquisa e veja se aparece algo.

Se um site de notícias tem vários comentários dando muitos elogios, tente curtir os comentários, tente enviar um comentário também, tente clicar em uma das outras notícias irrelevantes, tente clicar na logo, tente compartilhar (mas não compartilhe), tente clicar em "termos e condições". O ponto é que se você encontrar um botão que é só decorativo e não faz nada, você sabe que o site todo é mentira.

3.2 Não deixe nada passar.

Lembre a premissa.

> *"Por que este vídeo de 5 minutos continua depois de 1 hora?" "Por que esse jornal deixaria alguém vender algo no meio do programa?" "Por que não encontro registro dessa declaração em lugar nenhum?"*

Antes de qualquer ação, pare e recapitule. Se estiver prestes a fazer algo como:

> *"Vou pagar parcelado para provar que sou humano e liberar um trabalho onde aperto um botão que gera dinheiro infinito."*

Então algo está errado.

Capítulo 4

Senhas: regra que quase ninguém segue

Senhas fracas e previsíveis são fáceis de quebrar. Hackers costumam ter programas que às acham facilmente.

Evite:

- datas;
- nome + números;
- mesma senha em vários sites.

Uma recomendação atual é usar no mínimo três palavras distintas e desconexas.

```
escada_flor_17!
pato_lunar_198x
rioCobra!ventilador
```

[Não use literalmente estas.]

Gerenciadores de senhas são uma ótima alternativa. Eles, além de guardar suas senhas, podem gerar senhas fortes para você e evitar que você repita a mesma senha, dentre outros benefícios. Há um, por exemplo, dentro das configurações de uma Conta Google.

Uma regra simples para descobrir a segurança de sua senha é pensar: "Minha senha é facilmente memorizável?" Se sim, já é um pouco vulnerável.

Capítulo 5

Autenticação de dois fatores (2FA)

Autenticação de dois fatores (2FA[1]) significa que, além da senha, você precisa de um segundo elemento.

É frequentemente recomendado pois é muito comum que usuários tenham senhas que são comuns ou fáceis de adivinhar, que são usadas em vários sites diferentes, que vazaram ou que foram digitadas no lugar errado. É também uma medida preventiva.

5.1 Código por SMS ou e-mail

Adiciona uma camada a mais de segurança, porém não é infalível.

Existem desvantagens nesta opção.

No caso de um ataque direcionado, sabe-se que golpistas podem realizar uma clonagem de chip (SIM swap). No caso do e-mail, isso faz com que todas as contas dependam desse único ponto frágil. Também é bem fácil se enganar e passar os códigos secretos a alguém pedindo "verificação".

Apesar disso, é muito melhor que não ter!

5.2 Aplicativos autenticadores

São apps como Google Authenticator, Authy e Duo Mobile.

Eles geram códigos de verificação no próprio celular que duram poucos segundos antes de serem trocados. No caso de perda do celular dá para recuperar o acesso ainda assim.

Tem pouquíssimas desvantagens. São sujeitos só ao erro humano de colocar

[1] *"2-Factor Authentication" ou MFA, "Multi-Factor Authentication"*

os códigos no lugar errado.

5.3 Chaves físicas

Por exemplo YubiKey. Alguns celulares começaram a vir com essa opção integrada, senão pode ser necessária uma compra para adotar esta opção.

Com isto, posse de uma chave USB especial verifica a sua identidade. Algumas pedem até verificação de impressão digital. É um pouco mais difícil de recuperar no caso de perda.

Como elas verificam até legitimidade do site ou programa, é a opção mais segura. Contanto que conectar a chave para entrar na conta funcione bem para você.

Capítulo 6

Golpes envolvendo cartão

Tendo número, validade e CVV[1] já é possível fazer compras com um cartão.

6.1 Golpe da confirmação

"Insira todos os dados para confirmar sua identidade."

Usar um cartão para isso? **Nunca legítimo**.

6.2 Golpe da foto

Pediram fotos do cartão. **Nunca envie.**

6.3 Golpe do bloqueio falso

Uma mensagem chegou dizendo que o cartão "foi bloqueado" ou qualquer coisa parecida.

O objetivo é roubar seus dados.

Se *mesmo assim* acha que é real, nunca toque numa mensagem desse tipo! Abra o app do banco somente da tela de aplicativos, e nunca acesse o site do banco por um link/botão.

[1] *São os três digitos atrás. "Card Verification Value" ou VVC "Valor de Verificação do Cartão"*

Capítulo 7

Perfis falsos

Golpistas...

- ...roubam fotos de Instagram de conhecidos.
- ...criam perfis com mesmo nome.
- ...conversam por dias para ganhar confiança.
- ...usam IA para criar rostos e situações falsas.

O que fazer se suspeitar de uma conversa?

- Peça vídeo com um gesto específico.
- Peça um áudio.
- Pesquise a foto no Google.

É difícil ter certeza absoluta hoje em dia, mas pode ajudar.

Capítulo 8

Por que tudo isso acontece?

8.1 Só dinheiro

Dizer que algo está à venda, vender, não entregar nada e desaparecer. Pode ser simples assim.

Mas novidade é convencer alguém desesperado de algo que não é verdade, como por exemplo que folha de jequitibá cura a artrite, e entregar "a última folha de jequitibá disponível" de forma que a compra pareça legítima. Estratégias incluem citar cientistas reais com palavras falsas e artigos científicos totalmente sem relação. Acredite ou não na indústria de medicamentos, não significa que você deve acreditar em tudo que você escuta na internet.

8.2 Dados

Quando se faz compras em um site suspeito, é sempre possível que anotem sua forma de pagamento para uso próprio mais tarde.

Mas não apenas isso, mesmo sem qualquer transação, dados como nome, idade, CPF, até telefone e e-mail também podem ser usados para fingir ser você perante o governo ou seus familiares e amigos, o que pode causar danos sérios. Normalmente isso só acontece depois de um tempo, para que você esqueça que aconteceu ou para que um comprador seja achado.

E se você baixar algo e descobrir que não era legítimo, tenha certeza que removeu e então mude todas as suas senhas imediatamente, elas são muito fáceis de pegar.

8.3 Máquina

Baixando programas o risco é muito maior pois é possível conseguir seus dados sem que você os informe. Isso inclui ver tudo que você faz em tempo real.

Um propósito raro é tomar seus arquivos e fazer extorsão para você tê-los de volta. Contudo, **nunca vale a pena responder a qualquer extorsão**. Isso porque até os casos mais plausíveis quase sempre não passam de blefe e não há razão para crer que o outro lado cumprirá sua parte.

Outro propósito raro é juntar sua máquina uma botnet, um conjunto de várias máquinas que são cúmplices em derrubar sistemas alvo sem que seus usuários saibam disso. Também podem usar grande parte do poder de computação dos cúmplices para propósitos egoístas.

Capítulo 9

Como interpretar links encurtados

Links encurtados (por exemplo `bit.ly/...`, `tinyurl.com/...`, `cutt.ly/...`) são atalhos que escondem o destino verdadeiro.

Por mais que possam ser benignos, alguns podem até informar a quem te enviou em que cidade você mora, mesmo quando o destino é legitimo.

Se achar um, antes de clicar:

- use `https://unshorten.it/`;
- veja o endereço final antes de entrar.

Se o destino parecer estranho, não abra.

Capítulo **10**

Certificado TLS, o cadeado verde

Na barra de endereço de quase toda página que você visita você deve encontrar um cadeado, muitas vezes verde. Isso junto de texto e imagens convincentes podem te dar a impressão de que a página é um local seguro para colocar seus dados... Isso não é totalmente verdade.

O que significa:

- O dono e usuários do roteador não devem ter mudado a página que você está vendo;
- O dono e usuários do roteador não devem pegar o que você escreveu na página.

Não significa:

- que o site é oficial;
- que pertence a quem diz pertencer;
- que o site em si seja seguro.

Qualquer site pode (e deve) conseguir esse ícone.

Ainda assim, se um site não tiver o cadeado, não interaja. Como curiosidade, a seção a seguir explica por quê.

10.1 Explicando TLS a fundo. (Curiosidade)

O cadeado representa que há Segurança na Camada de Transporte (TLS[1]), portanto

1. usando matemática sabemos que a página que chegou é a mesma que o dono do certificado mandou;
2. uma certificadora autorizada (CA[2]) deu esse certificado a quem registrou o domínio (pode ser qualquer um);
3. o certificado não é muito velho.

assim garantindo que no transporte a mensagem não mudou.

Caso não haja essa garantia num site disponível publicamente, é possível que o dono do site tenha sido hackeado. Além disso, numa rede pública outros usuários podem acabar lendo o que você escrever. Seu navegador deve te avisar se esse for o caso.

[1] *"Transport Layer Security", havia uma versão antiga chamada SSL.*
[2] *"Certificate Authority"*