ARE MARCO DUES PAYMENTS SECURE OVER THE INTERNET? PUBLIC WI-FI?

DAVE LIEBERMAN, KT8E

I received comments recently that some members preferred to pay their dues by mail, citing concerns over use of internet – especially public wi-fi.

Over the past several years, the club has worked diligently to streamline the collection of club dues by managing online invoices. Tracking dues by checks, snail-mail and spreadsheets is a formidable and time-consuming task, wearing down the brave souls that volunteer for club secretary.

The online payment system has significantly improved the efficiency of tracking and collecting dues. But are we asking club members to take unwarranted security risks?

To have a conversation about browsing security, we first need to touch on two topics – Encryption and Phishing.

Encryption

By themselves, browsers are nothing more than digital data transceivers. The issue of security addresses **how** you send and receive.

If you submit forms in plain text, it is relatively easy for the amateur hacker to hack it with tools like WireShark. I teach a network class and show students how to do it. If you transmit encrypted data, it is still easy to hack but **impossible to decode**. With today's encryption algorithms it simply takes too long and requires too many resources to break it. The reality is encryption is a safe method of moving sensitive data across a public channel.

All modern browsers (Edge, Internet Explorer, Chrome, FireFox, Safari) can encrypt communications using SSL (Secure Sockets Layer) and TLS (Transport Layer Security) network protocols. In a nutshell, sniffing these packets results in capturing stuff like this:

```
/wEPDwUJNjU2Nzc2MDU4D2QWAmYPZBYCA
gMPZBYMAgMPZBYCAgEPZBYCAgEPDxYCHg
hJbWFnZVVybAVdLi4vdGh1bWJuYWlsLmF
zcHg/RmlsZU5hbWU9fi9Db21wYW55X0Rh
dGEvMTkvSW1hZ2VzL1BoeXNpb19TZWN1c
ml0eS5wbmcmV2lkdGg9MTAyNCZoZWlnaH
```

ASCII-Encoded encrypted data.

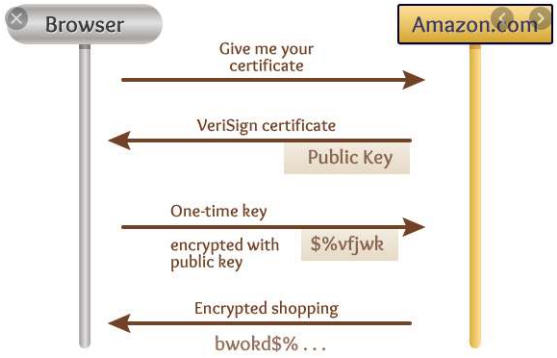
You can tell if your browser has established a secure connection if you see the padlock icon next to the name of the web site in the navigation bar. The full path to the web site contains the **HTTPS** prefix which stands for "Hyper Text Transfer Protocol Secure".

Secure connection icon

A web site cannot establish SSL connections (i.e. transmit securely) unless it obtains a digital "certificate". The certificate must be issued by a certifying authority (like VeriSign) that validates the identify of the domain-holder. Once an SSL certificate is installed on the domain's server, browsers that connect to that server exchange public and private "keys" to facilitate encryption. You can view these certificates by clicking on the padlock icon.

SSL Certificate for Google

The diagram below provides a high-level flowchart of the key exchange process. Sensitive data is not sent until the key exchange is completed. Sniffing the public key does not help the hacker – the server maintains a private key that is part of the decryption process.



Key exchange at start of connection

Phishing

Here is where most of us get into trouble with “secure” connections. You must pay attention to the actual **domain** that you are connected to. Even if the connection is secure, an untrusted domain puts you at risk.

Let’s take an example. I’m embarrassed to say this happened to me. I consider myself to be a computer “professional” but I fell victim to this scam.

THE BAIT

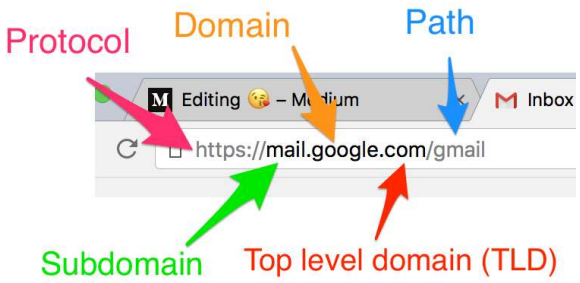
I got an email from “Netflix” that looks just like Netflix. It’s got their logos and artwork and even uses their font style. It says my credit card information expired and service is about to be terminated. My XYL is watching Netflix in the next room so I panic. I click on a link that says, “Go to your Netflix account”.

THE HOOK

The link didn’t go to Netflix. It went to a web site in “who knows where” that looks exactly like Netflix. It prompted me for Netflix login credentials and credit card information for renewal. I clicked Submit and nothing happened.

Congratulations! I managed to submit my Netflix password and credit card information to a phishing site. And I did it over a secure connection.

The moral of this story is – know who you are connected to. Keep an eye on your browser’s navigation bar and the address it contains. Here is a breakdown of an internet URL (uniform resource locator):



Internet web site address format

A domain may have many subdomains. For example, “http://maps.google.com” is a legitimate URL for google.com with “maps” as the subdomain. The MOST important part of the URL is the **domain** component.

Here are examples of sites with URLs that are intended to fool you:

```
registerdrivegoogle.sytes.net
netflixrenewal.A04113334222.zecure.com
fidelity-investments.4kqd3hmqgptupi3p.dozensby.loan
```

Note that these URLs have something familiar in the subdomain component, but the domain is NOT something you would normally recognize. Always double check and verify the domain component of your URLs to ensure you are browsing a trusted site.

Conclusion:

Are public wi-fi hotspots secure? IF you have the padlock (HTTPS) AND you trust the domain name (like WellsFargo.com) then **it is secure**. It doesn’t matter if you are at home on your cable internet or on the deck of a cruise ship over public Wi-Fi. It is the same encryption being used and **it is secure**.

References:

A Beginner's Guide to SSL: What It Is & Why It Makes Your Website More Secure
https://blog.hubspot.com/marketing/what-is-ssl

Transport Layer Security
https://en.wikipedia.org/wiki/Transport_Layer_Security

How does HTTPS actually work?
https://robertheaton.com/2014/03/27/how-does-https-actually-work/

How to Recognize and Avoid Phishing Scams
https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Is visiting HTTPS websites on a public hotspot secure?
https://security.stackexchange.com/questions/1525/is-visiting-https-websites-on-a-public-hotspot-secure

Wireshark – A Free and Open-Source Packet Analyzer
https://en.wikipedia.org/wiki/Wireshark
https://www.wireshark.org/