by Peter McCracken

A Primer to Being Safe Online

Discussion of research strategies rarely includes information about online security, but it's a topic worth learning about. The following suggestions are helpful when exploring the internet, regardless of what you're doing.

At **ShipIndex.org**, we receive payments for access to the premium database. We use **PayPal** for this process, so that we won't ever see customers' credit card information, but on rare occasions, people will send me a credit card number in an email, rather than go through PayPal. It's important to know that **an email has about as much security as a postcard**. Given the billions of emails that are sent every day, it's unlikely that someone will read yours—but on the other hand, if those with ill intent have a computer and get access to the nearly-infinite stream of emails flying around, they can easily write a program to search for sets of 15- or 16-digit numbers, which are most likely credit card numbers. By collecting that number and the information around it, they have a good chance at compiling valid credit card information. They can use it, or sell it to someone else. **Remember that it's always best to not send credit card information, or other personal financial information, in unencrypted emai**l.

Most email today is unencrypted. Encrypting email, both on the server (where it's sitting, waiting for you to read it) and as it travels to its recipient, is pretty hard to implement globally. Some of the largest email senders, such as Gmail and Yahoo!, provide encryption in transport, but both sides must use encryption for the system to work reliably. Without using an email encryption service, which can get complicated, it's pretty hard to ensure or expect that your email is secure while in transit.

If you want to avoid sending information by email, how do you know if websites or their online forms are safe? Many forms basically send information in an email itself, so just putting the information in a form is definitely not a guarantee of online safety. One important item to look for is when the URL (the web address) starts with **https://**, rather than **http://**. What does the '**s**' do? Does it really make a difference?

In fact, it does. The 's' is short for "secure" and defines a safer way of transferring data between your computer and the one that has generated the website you are viewing. The 's' denotes that both the sending computer and the receiving computer are using a technology called "secure sockets layer" and are sharing a special code that allows the information to be transferred in an encrypted manner. People or computers can still intercept the messages, but without the SSL key, the text is indecipherable.

Modern web browsers will show if you are using https://, usually by showing a green padlock icon in the URL bar. Note that a site that uses just **http://** isn't inherently bad, especially if it is just displaying information. The secure connection is most important when you are sending or receiving financial or private information through cyberspace.

Nevertheless, you may come across a URL in an email that looks ok, but isn't. Email software allows the sender to make text or URLs clickable. So the email might say, for example, "https://www.ebay.com/payments," but the people who created the email made the underlying link go somewhere else, where they'll then try to collect your payment information. (And they would probably do so securely, with SSL!) These are called "phishing" attempts; they try to trick you to go to a harmful site that might try to collect personal information or passwords, charge you fees, or download damaging software to your computer.

When you hold your mouse pointer over hot-linked data (*without clicking*), the email browser will show where that link would take you. It's important to be careful about such links, particularly in unexpected emails. Often the senders will pretend to be sending an invoice or a shared document; their real goal is to get you to click on the link or download the file that they've sent. A website called PhishTank, at **https://www.phishtank.com/what_is_phishing.php**, provides nice examples of phishing emails and webpages. These projects are not limited to online instances: scammers will sometimes call you on the phone, claiming to be the IRS about a supposed audit, or Microsoft offering to fix your computer. I know from experience that when the IRS audits you, they'll mail you a notification via the US Postal Service, and in no universe will Microsoft contact you to help you get your computer working faster.

The internet is filled with truly amazing resources and information, but it is also a resource targeted by people who try to take advantage of others, by stealing or misusing personal and financial information. Use the web, but be aware of what you see, and especially what you click on.

Suggestions for other sites worth mentioning are welcome at peter@shipindex.org. See **www.shipindex.org** for a free compilation of over 150,000 ship names from indexes to dozens of books and journals. ⚓