

Watch Out for Bogies When You Hit the Links

October 2011



Dreaming about getting away from where you are now and playing a few rounds of golf with your friends and family? Before you hit those links, here are some other links to think about that aren't so friendly. The bad guys are getting pretty sophisticated in their phishing scams and the way they disguise embedded links in emails. Copying artwork and other identifying elements and language off of legitimate web sites are now standard practices. Usually it is still relatively easy to spot phishing scams from foreign countries because of the bad grammar and spelling used in them. But online scammers have continued to improve and may have even taken a few English classes. The results are new phishing attempts with potentially dangerous links that are harder to identify and dismiss at first glance. That puts the unwary recipient – like a tired soldier or a family member who is not cyber savvy – at risk.

Most of us can see through classic scams like the foreign finance minister or businessman who wants your help getting money out of his country. It should also be safe to assume that everybody knows not to download or open attachments in emails from unknown or unexpected senders. But embedded links in emails that appear legitimate are some of the toughest traps to spot. Here are a few tips to help you avoid losing any personally identifiable information (PII) and downloading malware due to well disguised bogus links.

Often telltale clues as to whether a link is good or not are in the link itself. Pay close attention to what comes just before the ".com." That information identifies the true name of the linked site. It is very easy to create a sub-domain name that sounds official. A classic example of this is an email saying there is a problem with your bank account and that it has been temporarily closed for your protection. To reactivate the account you must follow the link "citibank.acctvalidate54.com" and provide PII. Looking closely at that link you will notice that the actual domain name is acctvalidate54.com and not the Citibank site. This use of sub-domains to disguise a dangerous website is a very common trick used in phishing attacks.

To be completely safe, simply never follow a link in an email. However, if you do follow email links, only use links embedded in emails from sources you know are legitimate. For example, over time you learn to recognize the little details of emails from trusted senders. While phishing techniques are getting better, they rarely include all of the details that identify a trusted email. Even spear phishing attempts - scams using public or stolen personal data – rarely can get everything right. Often it is the tone and content of the email that gives it away as a scam. Typically an email needs you to follow a link to resolve an unexpected problem or to take advantage of an opportunity in a very short time frame is potentially dangerous.

One common technique for avoiding potential bad links is to retype the URL into your browser. That ensures that a cleverly disguised fake link can't take you to another site. Also, you can often tell if an email link is legitimate by mousing - pointing at the link with your cursor but NOT clicking any of the buttons - over the link. Make sure that the link that pops up matches the link in the email exactly. The word "exactly" is very important here, because the slightest variation in the address could lead to a risky site. Another technique is to use a trusted link that you have saved in your browser, if you have previously identified it as a legitimate link. In addition, due to the new security elements that major search engines have put in place over the past few years, they have become a reliable tool for obtaining valid addresses.

Again, following a link from a email that tries to scare you into immediate action like a financial account closure or any link that promises something that is too good to be true is usually a sure fire way to get in trouble. Even then, pay close attention to the details in a link, because the bad guys are betting you won't. They are also betting that you won't pass this advice along to friends and family. Just something to consider before you next hit the links.