Phishing

No, the title of this newsletter is not misspelled. Phishing is indeed a word, and according to Wikipedia it means "the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication."

There has been a lot of news lately on major websites getting hacked (the most recent being eBay just this week). By now, you hopefully know how to create a strong unique password (if not, please see my previous newsletters on this subject) and that when a site is broken into, to quickly change your password. Unlike an attack on a major web site, phishing is an attack on you personally. I was subject to a phishing attack just this week (which I did not fall for), so I thought I would use this month's newsletter to discuss what happened.

Here is the phishing email I received (the name is changed):

> Joe Smith
> To: undisclosed-recipients
> Bcc: Steve Gimnicher (steve@gimnicher.com)
>
> Kindly view this newsletter i uploaded for you using Google Docs secured File uploader, To view open: Continue and sign in with your email for your secure access, it's a very important news.
>
> Best regards,
> Joe Smith

"Joe Smith" is indeed someone I know (my neighbor) and in inspecting Joe's email address (by clicking on it in the email), Joe's email address

was legitimate. When I placed my mouse over “Continue” to view the link, I saw http://segurizimo.com/googledocs2014hyb/gdook/ which told me right away that this was not a legitimate link. A legitimate link would have started with www.google.com. I was fairly certain that if I clicked that link, it would have asked me for my Google account email address and my password. It turns out that other neighbors received this same email, and one of them fell for it, entering his Google account password. Now the perpetrator of this email had my neighbor’s login credentials, including his actual password. With this information, in addition to being now able to send the same email to all of this neighbor’s contacts, the perpetrator could try the same login credentials on all the popular websites, and might be able to get access to even more information. My neighbor called me, and I told him to immediately change his Google password and any other account that had the same password and to watch for any suspicious activity in any of his online accounts. I also contacted “Joe Smith” to tell him that his email was hacked, that probably all of his contacts received this email, and to change his email password immediately and let all of his contacts know not to fall for this phishing attempt.

There are so many benefits to being on line, but one has to be very cautious. If an email looks suspicious in any way, especially if it has an attachment or includes links, ask yourself if the sender would really be sending this to you. If it looks “phishy”, contact them to verify they sent it before proceeding further.

As always, I hope you have found this information useful. If you do not wish to receive these emails in the future, let me know.

This newsletter, as well as all past newsletters, can be found on my web site (http://steve.gimnicher.com).