Cybersecurity Presentation – Miscellaneous Notes and Commentary

by Rich Cacace

Thanks so much for attending our presentation. I hope it was helpful to you. I have created links to all the material Rob discussed, including the labs. Please feel free to share this with friends and family. The more aware people are, the harder it is for hackers.

There was a lot of interest in "password vaults", aka password managers. Rob uses Keeper Security, while I use Last Pass. Despite what the link indicates, I've been using Last Pass for free for several years. There are some limitations, but I've had no problem using it on multiple computers and my phone and still haven't been charged. I highly suggest reading this CNET article and doing some research to see which would work best for you.

As I mentioned to some attendees after the presentation, Rob and I have different approaches. He is talking as a cybersecurity expert, so he's telling you what to do to maintain the highest level of security. It's akin to having a security consultant telling a bank how to secure a vault. I personally feel that you can take a more pragmatic approach and still be very secure. Remember, if a hacker has to work to break in, s/he will move on to an easier target.

With that in mind, here's what I think you should consider:

1. Keep a different password for each "high-value" account (banking, insurance, stocks, etc.). This way, if one is compromised, you can feel safe knowing that the others aren't going to be easy targets.
2. Follow Rob's advice on using a phrase that has meaning to you, but substituting numbers and symbols. While a 24 character password may be ideal, it's very, very unlikely you'll have problems if it's less. When I was in the military, the requirement was 14 characters, so I'd go with that.
3. I personally don't see an issue with using passwords for multiple sites, as long as the password is difficult to hack and the site doesn't have information that is very important.
4. As to changing passwords, again, I'd change "high-value" sites more often.
5. I never store my credit card information on a site. Places like Home Depot, Target, Walmart, etc. are often hacker targets. If they break in, your credit card will be compromised.
6. I never use a debit card for online purchases. Although the card is insured like a credit card, that money is being taken directly out of your banking account. I had one student who's debit card was stolen. She lost everything and even though she would eventually get the money back, she had mortgage and other bills she could not pay.
7. Don't EVER click a link or attachment from an email, even if it appears to be from someone you know. Always type in the place it's purported to come from.

I hope that helps. Please feel free to email me at rcacace@pensacolastate.edu or Rob at rpratten@pensacolastate.edu .