About Listserv security:

Question:
Hi. I joined your group during the recent scion exchange. I thoroughly enjoyed myself at the event. Everybody was so nice and friendly and helpful in answering all of my questions. I look forward to attending future events. I also understand that there have been a few accounts that have been hacked. Are these isolated incidents or do others within the group need to be concerned? I do have some protections on my computer, but I did open one of the links on X's e-mail the day before the report on her acct. getting hacked was announced. Could someone please discuss the hacking incidents a little bit more?

Answer:
The CRFGR website is relatively safe from hackers, spammers, and viruses. But no one is 100% immune; not even the government and big companies.
I think we have been getting about 2-3 spams a year slip through.

First, we orchardists are a relatively value-less demographic to commercial hackers, so rarely pursued in my experience.

Second, our GoogleGroups structure protects us in a few ways.
When an obvious piece of spam comes into the group, our mail-masters can merely delete that sender's email address as an allowed participant, and notify the sender to register & use an alternate email address.

Third, our CRFG group is very topic-specific. Use a little common sense when you get an email with a "nonsense" subject line, nonsense content, or just a url hotlink as content. Treat it as spam. Either delete it (the best idea), or use the "doubled asbestos glove" method of first turning on your browser's version of "private browsing", then opening the suspicious link by using a proxy-server like proxify.com or anonymizer.com.

Fourth - all officer, committee, and activist's email addresses on the chapter website are modified to not be able to be harvested by spam bots, so can't be used to spam the listserve.

Fifth, users need to practice safe computing.
Use a virus detector. You can probably get it free from your internet service provider, like Norton from Comcast http://xfinity.comcast.net/constantguard
Don't use free wifi hotspots without passwords and security login software.
Put a password on your own home wifi
More safe computing tips at
http://askleo.com/internet_safety_8_steps_to_keeping_your_computer_safe_on_the_internet.html

I have been getting increasing spam from compromised email address books from friends, family, clients and colleagues.
This appears to be mostly from people using online email, like yahoo, google, hotmail, aol, etc wherein the address book is stored online, not on the victim's computer!
This is the source of the occasional spam that the CRFG email group has been experiencing.
The hacker has gotten into the victim's email address book online, and sent an email to all email addresses in the victim's online email address book. Any email address that works will continue to get spam from that sender's email address.
This is why we can turn that kind of spam off so easily. We just unsubscribe that sender's email address,

but unfortunately they will need to use a different one to use CRFG listserve. They can still use their other email for everything else.
For example, I have one email address for personal use, that I use for CRFG. If I try to send a message with any of my business email accounts, the email bounces back to me and does not get through.

Good email account passwords are a key to computer security to keep your address book from being hijacked.
This article gives a good background and solution.
http://ask-leo.com/how_do_i_choose_a_good_password.html
Skip to the end if its too boring for you, or skip the link and just do what he says:
"The single most important thing you can do to improve your password's security is to make it longer."
A 12-character password results in 19,408,409,961,765,342,806,016 possible combinations.
And, bonus: it's extremely unlikely that a dictionary attack will bother with the assorted combinations to eventually get to whatever it is you put in 12 characters.
Length doesn't imply complexity. There's a very strong argument that says:
****password**** is a significantly more secure password than 7CxX&*Xf
In fact, even longer pass phrases – something like perhaps:
correct horse battery staple or mydogeatsmyfroot (note the one mangled word & which doesn't require screen change on a smartypants phone) are perhaps best of all.

So, what should you do?
Abandon eight-character passwords. They should no longer be considered secure.
Create all new passwords 12 characters or longer. (You can make a password longer and more secure by adding repeating characters if you can't think of anything else.)"

Also, Macs are now under attack by visiting links carrying Trojans, and fake high-ranking sites on search engines are increasingly carriers:
per symantec security http://www.symantec.com/threatreport/topic.jsp?id=threatreport&aid=conclusion
"In 2011, malicious code targeting Macs was in wider circulation as Mac users were exposed to websites that were able to drop trojans. This trend is expected to continue through 2012 as attack code exploiting Macs becomes more integrated with the wider web-attack toolkits."
--
Keith
webmeister CRFG-Redwood.org