

California Computer Care

News,
Views,
Tips and
Cool Techniques
for CCC Members

November 2006
Vol. IX, No. 11

We
speak
Geek,
so you
don't
have to.

Beware of Phish

The bad guys do not give up! Since the late 1980s, the bad guys of the computer world have been trying to hurt the rest of us. Way back then, virus writers wanted to vandalize our machines with nasty, mean spirited *practical jokes*.

In the 1990s, the bad guys turned from vandalism to competing for the title of *Baddest of the Bad*. Viruses mutated into worms, and the internet came close to imploding.

By the late 90s, the profit motive entered in. The bad guys discovered that they could take over innocent computers without anyone knowing. These computers became *zombies* directed to do the bad guy's bidding by spewing spam across the internet. By using other people's computers and email accounts, they avoided detection and gained free access to the internet. Every piece of spam that motivated a foolish recipient to click a web link earned the *zombie* masters a few pennies. Since billions of spam emails are sent, the pennies add up tidily.

And then there was *Spyware* that sneaked onto your computer and watched your every move and reported what you did to the bad guys. Every password you sent, every credit card transaction, every secret told could be captured by bad guys and used to rob you.

Related to *Spyware* is *Adware*. Software that is put, unknown to the user, on their computer. *Adware* hijacks the web browser and takes users to advertisements that they never asked to see or to web sites that they never requested in an avalanche of browser windows opening without any way for the user to stop them!

The attacks have been relentless. Countermeasures are devised, but the bad guys defeat each and every one. Businesses were created that sell products just to stop *Adware*. Now, organized crime has joined in as well.

Hooray for Macs! While we Mac users were sometimes victims of the vandals of the 80s, we have not been affected by these newer and far more dangerous threats. No Mac has ever been a *zombie* or been afflicted with *Spyware* or *Adware*. Those are strictly *Microsoft Windows* diseases.

It isn't magic that protects us, but good software design. *Mac OS 8* and *9* put an end to the vandals. *Mac OS X* handily turns back all outside attempts at takeover. This is both by design and as a result of a difference in philosophy.

Microsoft Windows (and *MSDOS* before it) was designed with corporate control in mind. The Microsoft way was to give all power to IT technicians. *Windows* is designed so that a company's computer technicians can take over a user's machine without their consent or knowledge. That computer can then be changed in any way that the technician likes or needs even if that is a detriment to the user. This power, once bequeathed, is not revocable and so the bad guys discovered that they can use the same means to attack computers as though they were technicians with the right to do so.

Apple, a company of iconoclasts, started with a different philosophy in mind. They put all power in the user's hands. Therefore, in order for a technician to take over your Mac, they need your permission. With *Mac OS X*, this has manifested as a rather paranoid computer that is constantly looking for threats and asking for the user's password when it feels insecure. Such behavior is a bit annoying, but it keeps us safe!

Is it any wonder that the corporate business world wanted nothing to do with desktop computers until IBM and Microsoft offered them machines that would be the perfect corporate slaves that they desired?

You are the supreme power to your Macintosh. That is why you have a user account and a special user name and password. So far, the bad guys have not found a way to circumvent your Mac's need for your OK when they try to attack. If all goes well, they never will.

That is, unless you help them. New threats have arisen that rely on you for their success. These threats are referred to as *Social Engineering Attacks*. Clever bad guys are trying to get you to approve their nasty plans. They appeal to greed: "Click here for free music!" They appeal to sex: "Naked pictures! Click here!" They appeal to

good citizenship: “Click here to support our troops.” And more. The worst of these attacks are cutely called *Phishing Scams*.

A fisherman drops a hook in the water and hopes a fish takes the bait. The fisherman would have better luck if he could drop a thousand hooks in the water simultaneously. A *phisher* does the same. He sends out millions of emails and waits for an unsuspecting *phish* to take his bait. The *phisher* doesn't bait with worms, but with fear. A typical *phishing* email will look like a message from your bank. All of the usual attributes are present, bank logo, address, link to the bank's actual web site, etc. The message will look absolutely genuine. It will inform you that someone has illegally accessed your account. The account is now on hold. Please click this link to go to a special web site where you can verify your ownership of the account. Once there you are asked for your account number, social security number, secret question (Mother's maiden name?), passwords and so forth.

But it isn't your bank at all. The *phisher* has posed as your bank. There is nothing wrong with your account and the *phisher* knows nothing about you. That is until you give the *phisher* all of your account information. In a flash, your bank account is emptied and your identity is stolen.

No legitimate business will ever ask you to provide vital information in this way. Never respond to any email request that takes you to a web site that asks for any of your personal information. Ever!

Phishers can also attack you by sending you to an innocuous web site such as a *MySpace* page and

while you look at the page, they will suck your passwords out of your web browser.

Both *Safari* and *Firefox* store passwords when you visit web sites. This is an attempt to be helpful. The next time you visit that password protected web site, *Safari* or *Firefox* automatically sends the password so that you are not bothered to do so.

But the *phishers* have found a way to secretly force *Safari* and *Firefox* to divulge the passwords that they know. When this happens, you will see nothing at all and be unaware. Fortunately, this is a new technique that hasn't had time to victimize many innocent people.

The fix for this attack is simple though inconvenient. You must turn off *Safari* and *Firefox*'s ability to store passwords. Here's how:

For *Safari*—

- 1) From the *Safari* menu, choose *Preferences...*
- 2) Click the *Autofill* button.
- 3) Uncheck the check box next to: *User names and passwords*.
- 4) Close *Safari Preferences*.

For *Firefox*—

- 1) From the *Firefox* menu, choose *Preferences...*
- 2) Click the *Security* button.
- 3) Uncheck the check box next to: *Remember passwords for sites*.
- 4) Uncheck the check box next to: *Use a master password*.
- 5) Close *Firefox Preferences*.

You will now have to manually enter passwords.

These simple changes will help to keep you safe.

But, your vigilance is still needed. Always be

aware of where you are on the internet. Don't be fooled into revealing important information or following suggestions from strangers.

If you have questions about an email or web site, please contact me before you proceed.

Thank you and be safe.

Happy Holidays!

November Tip—

While you are changing *Safari Preference* settings, you may want to make another change to help your security.

Safari will automatically open downloaded files without asking your permission. This could be exploited to attack you. So, it is wise to turn this feature off. Please do this:

- 1) From the *Safari* menu, choose *Preferences...*
- 2) Click on the *General* button.
- 3) Uncheck the check box next to: *Open "safe" files after downloading*.
- 4) Close *Safari Preferences*.

California Computer Care

P.O. Box 9445

Santa Rosa, CA 95405

(800) 540-8989

Like an
auto club
for your
computer.