Keeping Sunningdale's Computers Virus-Free

Ed Cloutier, Sunningdale Golf & Country Club

Sunningdale's computer system is a vital part of our business operations, and we all need to do our part to ensure we use the computers we are given in a prudent way to keep our network safe.

Threats To Watch Out For

The most common way for our network to be attacked is by getting one of our own staff to "let a bad guy in" accidentally. The most common ways this happens are:

- **Opening an email that has a virus as an attachment**
- **Visiting and infected website on the Internet – email links**
- **Visiting an infected website – via search engines**
- **Installing "freeware" software from an outside source**

Here are some tips to help avoid falling prey to one of these techniques.

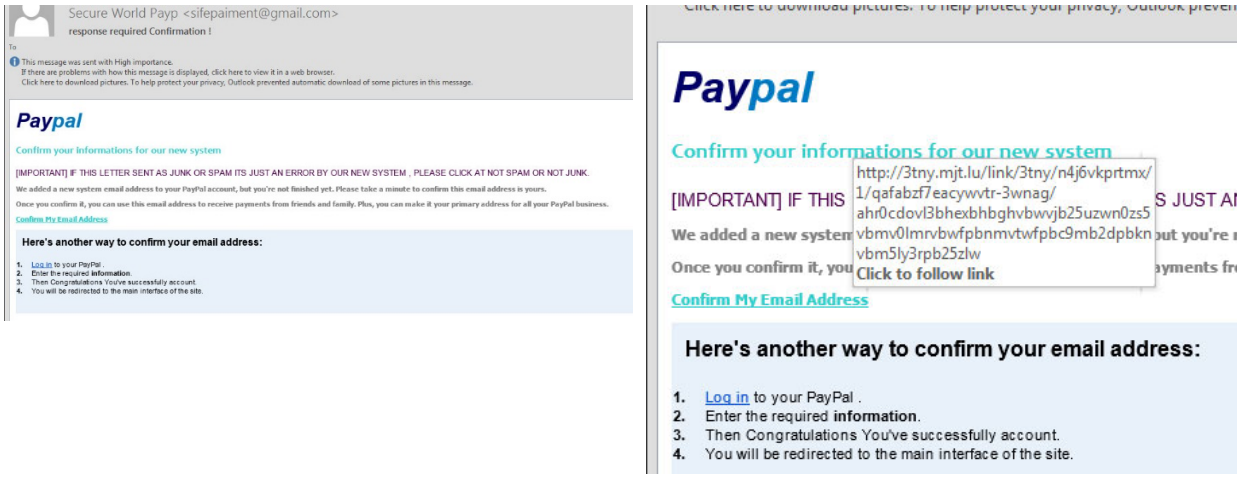
Avoid Opening Email Attachments You Don't Know: typically, emails themselves can't hurt our network, but the things they carry CAN HURT US if they are "launched" (opened) by someone logged into our network at the time. As for attachments:

(1) If the email is not specifically to you or if it is from a source you don't know or didn't request, DON'T OPEN IT.
(2) If the attachment is within a ZIP archive which makes you open the ZIP before you open the attachment, DO NOT OPEN EITHER (this is a very common technique to get a virus past anti-virus software checking)
(3) If the email is "plausible" (eg. It is from FedEx and you were indeed waiting for a courier package), be VERY CAUTIOUS and look for signs that it is directed to you or is from the source you expect. If the message is "generic" and doesn't include any directly-identifiable information about the sender or the package itself, DON'T OPEN IT.
(4) If the email is from a large company (Microsoft, eBay, Royal Bank, etc), be aware that these organizations do NOT generally send out attachments on their messages … and actually rarely send out any emails to individuals. DON'T OPEN IT.

Visiting Infected Websites on the Internet – email links: A link inside an email can open the door to viruses by taking you to a bogus or infected website. As mentioned above, one common way to "lure" you to an infected website is to send a "link" in an email message that makes you think you are going to Rogers, Bell, Kijiji, FaceBook or some known site but will actually take you somewhere else. Here are a few general tips to remember when looking at "links":

- Be aware that the WORDS of the link that are visible may not match the actual website's address that it is taking you to. For instance, I can make a link that visibly says "rogers.com/support" but will have an underlying target address of something totally different! If you "hover" your mouse over a link WITHOUT CLICKING IT, it should pop up the underlying target, which is one sure way to spot a bad link.

Here is an example of an email that has a “click” that does not go to where it might appear. The item on the left appears to be an email from PayPal (which you might actually have), and it has a link in it to login to PayPal. However, when I “hover” (without clicking) my mouse over the LOG IN link, I can see in the popup the REAL address it wants to take me to , and this is DEFINITELY NOT PAYPAL.



What should you do if you got this PayPal email or anything like it? First, realize that PayPal would not send such a thing (especially with such atrocious grammar and no personal acknowledgement of who it is going to). Second, if you wanted to check, USE YOUR OWN BROWSER TO GO TO PAYPAL’S HOME PAGE and login on your own – do not use the link in the email. Then, DELETE THE EMAIL ASAP.

- Be careful of an “extended” link: Bad Guys will make the first part of a link look legit … but then “extend it” with things that will actually take you someplace else. For example, you might see a link that looks like www.bellcanada.customerservice.client.ontario.rstqx.ru/help - this link is going to a server called rstqx.ru (which is in Russia), even though there are a lot of references to Bell Canada on the front. Tip: look for the first “slash” (i.e. “/”) – whatever is JUST BEFORE THAT is the actual site’s name.

Visiting Infected Websites via Search Engine: many of the same techniques as in email links are used by Bad Guys when you use search engines like Google, Bing or Yahoo to search for websites. Remember: **Google doesn’t always know a real website from a bad one**, so be cautious about where you go based on a Google search result.

How do the bad guys get on Google’s front page? Many of the first items on a search list are actually PAID ADS, and there are many examples of Bad Guys having paid for ads that are tied to certain popular key words and take you to virus-laden websites as the results. This is particularly true in fast-moving social networking or “current news” areas.

For instance, say a celebrity was arrested – there will be a flood of Google searches on that celebrity’s name by curious people wanting to find out what happened. This is a perfect time for a Bad Guy to put up a website that “looks” like a fan page for that celebrity but is actually a site that wants to install a virus on your PC. That Bad Guy may flood google with fake “hits”, making Google think their page is

"popular", or they might buy that celebrity's name as an advertising link. Both will lead unsuspecting "clicks" right to them.

How do you avoid going to an infected website?

- Avoid links in emails or on webpages that purport to bring you to popular websites like cnn.com or ebay.com – if you want to see what CNN has to say, GO DIRECTLY TO CNN.COM yourself and do a search of their site.
- In general, find a number of respected website you use to get information (TSN for sports, CBC, CTV, lfpress.com (London Free Press) or Global for news, theweathernetwork.com for weather etc. Then, bookmark these and go to them yourself – don't follow a link someone sends you or trust a google search that wants to bring you to these know sites. If you want to know how Tiger did at the Masters, go to MASTERS.COM – DO NOT GOOGLE FOR TIGER WOODS, which might bring you to a bad place.
- REALLY avoid links in emails that come from what appears to be a friend or acquaintance that seems to say: "Here's a good joke" or "Check this out". This is truly bad behaviour and any links you receive at work like this should never be followed while at work.

Installing FREEWARE Software from an Outside Source: Sometimes, there is something you'd like to do at work that your computer doesn't do, like viewing certain video file types, or editing certain images or documents, or something else. Using Google to search for programs to solve your problem is a common way viruses get installed.

- In general, DO NOT INSTALL ANY SOFTWARE ON A PC AT WORK. If you need to do something that your computer doesn't do, please contact Ed Cloutier at ext 231 to inquire about the way to get what you need done.