This month I am going to share a few emails whose purpose was to deliver a virus and also briefly discuss email spam. My purpose in doing so is to make you aware of these techniques so that you do not fall prey to them.

Email Viruses

The first email, shown just below, was actually received by one of my customers (I blacked out the address to protect his privacy). This email is especially devious because it looks completely legitimate. With the email came an attachment presented to look like a printing label. As you read through this email, you will see that it directs you to print the attached label. Upon opening of the attachment in order to print it, a virus was installed which performed considerable mischief on the computer, rendering it fairly useless and requiring several hours of my time to rectify.

Subj: **Delivery information contains at the postal label**
Date: 4/21/2012 1:40:52 P.M. Pacific Daylight Time
From: parcel@usps.com
To: [redacted]@aol.com
Postal notification,

Your parcel can't be delivered by courier service.
Status deny\It's not right the address of recipient.

LOCATION:Albuquerque
PARCEL STATUS: sort order
SERVICE: Express Mail
NUMBER OF YOUR ITEM:U839489746NU
INSURANCE: Yes

The label of your parcel is enclosed to the letter.
Print a label and show it at your post office.

Attention!
If the parcel isn't received within 30 working days our company will have the right to claim compensation from you for it's keeping in the amount of $5.77 for each day of keeping of it.

You can find the information about the procedure and conditions of parcels keeping in the nearest office.

Thank you for your attention.
USPS Express Services.

One of the most important guidelines to prevent viruses is to never, ever open an email attachment if you aren't 100% certain that it is legitimate. In this case, if you wanted to test the legitimacy of the email, rather than opening the attachment, one could simply call USPS to authenticate the item number.

The next example below was actually sent to me. I am an Amazon customer and I do make purchases on Amazon. As you will notice, the canceled order number appears as a web link. In this case, I knew that I hadn't cancelled an order, but if I didn't know better, I might still have clicked the link out of curiosity. Another way to check if a link might lead to a suspicious site is to just place the mouse pointer over it and pause for a few seconds. Generally, this will cause the actual link to be displayed. When I did that, hovering over the order # 12-1853-76449, caused this to be displayed: "http://118.45.190.188/~nice/adjudicated.html" The same appeared when I hovered over "http://www.amazon.com" at the bottom of the message. A link of this form generally will lead you to a site that is up to no good. Another technique to use if you are concerned that a legitimate looking link might not be, is to instead of just clicking the link in your email, opening up your web browser and typing the link address explicitly.

From: "order-update@amazon.com" <order-update@amazon.com>
Subject: Amazon.com - Your Cancellation (12-1853-76449)
Date: May 2, 2012 11:32:37 PM PDT
To: "gimnicher@aol.com" <gimnicher@aol.com>
Reply-To: "order-update@amazon.com" <order-update@amazon.com>

Dear Customer,

Your order has been successfully canceled. For your reference, here's a summary of your order:

You just canceled order 12-1853-76449 placed on May 3, 2012.

Status: CANCELED

---

1 "Limits"; 2003, Deluxe Edition
By: Teresa O'Sullivan

Sold by: Amazon.com LLC

Thank you for visiting Amazon.com!

Amazon.com
Earth's Biggest Selection
http://www.amazon.com

Finally, one more example, also sent to me:

From: "Chase Notifcation"<189230211@custhelp.com>

Subject: Unable to verify your account details

Date: May 24, 2012 1:08:05 PM PDT

1 Attachment, 23 KB

Dear Chase Bank customer,

This e-mail has been sent to you by Chase Online to inform you that we were unable to verify your account details. Our technical service department has recently discovered that your information on file with us is incomplete.

Please confirm that you're the owner of the account, and then follow the instructions, download the attachement form and follow the steps to open a secure browser window.

Regards,Chase Online member services.

Personal.Update.htm (23 KB)

I know that Chase would never send me an email like this, and they certainly would not use a reply email address containing "@custhelp.com". The attachment ("Personal.update.htm") if clicked would install a virus.

Email Spam

Another email problem is spam. Most modern email clients and servers have spam detection and filters built in, but I do want to mention a couple of points regarding spam. The first is that you should not unsubscribe to emails from sources that you have not conducted legitimate business with. The reason for this is that when you unsubscribe, the spammer now knows that your email address is active and valid, and your spam will likely increase. For the same reason, never click any links or pictures contained within the spam. Many of these will have code in them that alerts the spammers that the email has been opened. Also, never purchase anything from web sites that you were directed to via spam. If they are spamming you, they are not trustworthy, and you should therefore not give them your personal information.

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 (www.gimnicher.com/steve).

Steve Gimnicher
Gimnicher Computer Services
www.gimnicher.com/steve
650-222-4140
steve@gimnicher.com