IN THIS ISSUE:
~ Email Issues

COMING NEXT MONTH:
~ Wireless Broadband

READY NET GO … NEWS

July 2007 **http://www.readynetgo.net** **610-856-0990**

Tips of the Month

Country Domain Extensions

You'll see the following extensions on website addresses as well as on email addresses. Many spammers and phishers reside outside the US. Become familiar with international extensions so you can recognize SPAM and phishing sites on the web.

Sample list of domains by country:

.au -	Australia	.nz -	New Zealand
.cn -	China	.ru -	Russia
.de -	Germany	.tw -	Taiwan
.jp -	Japan	.uk -	England

For the full list of domains by country see: http://www.iana.org/root-whois/index.html

……………………………………

Faulty Dell Displays on Notebooks

Certain models of Dell notebooks are being fixed at Dell's expense due to vertical lines that may appear on the screen. If you have noticed a problem with the display on your Dell notebook, contact Dell to resolve the issue.

Dell's blog (link below) provides information on the models affected; reference the blog when you call. Those who already replaced their screen may be eligible for a refund.

http://direct2dell.com/one2one/archive/2007/06/19/17774.aspx

……………………………………

PA Renewable Energy Festival [9/22]

WIN a 2007 Toyota Prius – visit: www.paenergyfest.com/hybrid.shtml

Email Woes Got You Down?

Tips for deciphering confusing email messages

Have you ever received a message from yourself or an undeliverable message notification that doesn't make sense? Do you get emails from banks and credit card companies asking you to verify your information but you don't have an account with that institution? Ever received a domain renewal email even though you just renewed?

These are all examples of **SPAM** and **phishing messages**. Security and identity theft are becoming enormous issues. In this newsletter, we'll show you real-world examples of SPAM and phishing emails so you'll be able to recognize these messages when they show up in your Inbox.

First Things First

In this day and age, to avoid headaches, **treat EVERY email message as if it were malicious**. This includes emails that come from co-workers, family and friends. Keep in mind that an email may appear to come from someone you know, but it actually originates from someone else.

Another concept to grasp fully is that spammers send out hundreds of thousands of emails to individuals around the world. They don't know you and they don't care about you – all they want is money. Don't take SPAM or phishing emails personally, EVERYONE receives "unsolicited email" – just be aware of these messages and delete them.

SPAM and phishing emails are not going away anytime soon so we all must BE VIGILANT, become educated and work with the controls we have available such as email filters.

WWW (Websites Worth Watching)

Become an expert "phish" detector by visiting these sites:

1. www.chase.com –Click on **Online Fraud and Email Scams** (lower left) and then click **Example Messages** under Related Links (on the right side of the page).
2. www.citicards.com – On the main navigation, click **Security & Privacy** then **Site Security**
3. www.ic3.gov – Click on **Press Room** for examples

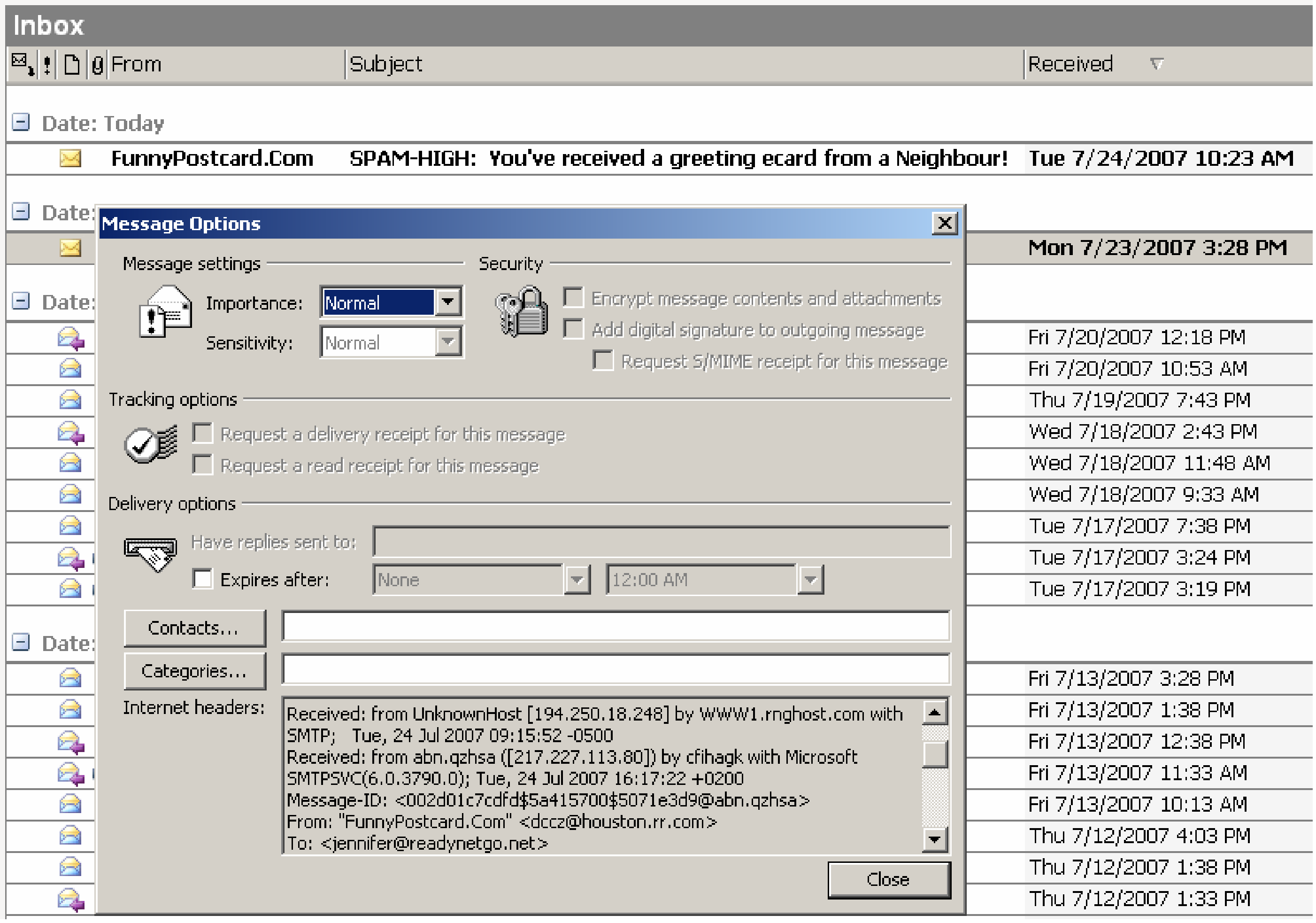
How do I detect SPAM?

Most of the time, as you are scanning your Inbox, the subject of the email is a dead give away. **Nonsensical or inappropriate phrases should be discarded immediately**. Other phrases such as "Online Banking Form", "Update your Account Information", or "Just take a look" are huge red flags.

Another tactic spammers use is to replace letters with numbers like "V1agra" for "Viagra" or "Amb1en" for "Ambien". SPAM filters are configured to flag common words so spammers will transpose letters or use numbers to bypass the filters.

If you're not sure if the message is SPAM, look at the **Headers** of the email before opening it. All email messages show routing information including who is sending the email, the ISP (Internet Service Provider) it comes from, and general date & time information. To view the headers of a particular message in Outlook 2003:

1. Right click the email message
2. Scroll down to **Options**
3. At the bottom of the dialog box you'll see a section called **Internet headers** like *Figure 1* below:


Inbox
From
Subject
Received
Date: Today
Date:
Date:
Date:
Message Options
Message settings
Security
Encrypt message contents and attachments
Add digital signature to outgoing message
Request S/MIME receipt for this message
Tracking options
Request a delivery receipt for this message
Request a read receipt for this message
Delivery options
Have replies sent to:
Contacts...
Categories...
Close

From	Subject	Received
FunnyPostcard.Com	SPAM-HIGH: You've received a greeting ecard from a Neighbour!	Tue 7/24/2007 10:23 AM

Importance: Normal
Sensitivity: Normal
□ Expires after: None 12:00 AM

Internet headers:

```
Received: from UnknownHost [194.250.18.248] by WWW1.rnghost.com with
SMTP;   Tue, 24 Jul 2007 09:15:52 -0500
Received: from abn.qzhsa ([217.227.113.80]) by cfihagk with Microsoft
SMTPSVC(6.0.3790.0); Tue, 24 Jul 2007 16:17:22 +0200
Message-ID: <002d01c7cdfd$5a415700$5071e3d9@abn.qzhsa>
From: "FunnyPostcard.Com" <dccz@houston.rr.com>
To: <jennifer@readynetgo.net>
```

Mon 7/23/2007 3:28 PM
Fri 7/20/2007 12:18 PM
Fri 7/20/2007 10:53 AM
Thu 7/19/2007 7:43 PM
Wed 7/18/2007 2:43 PM
Wed 7/18/2007 11:48 AM
Wed 7/18/2007 9:33 AM
Tue 7/17/2007 7:38 PM
Tue 7/17/2007 3:24 PM
Tue 7/17/2007 3:19 PM
Fri 7/13/2007 3:28 PM
Fri 7/13/2007 1:38 PM
Fri 7/13/2007 12:38 PM
Fri 7/13/2007 11:33 AM
Fri 7/13/2007 10:13 AM
Thu 7/12/2007 4:03 PM
Thu 7/12/2007 1:38 PM
Thu 7/12/2007 1:33 PM

Figure 1. Common SPAM message from FunnyPostcard.Com. Right click the message and choose Options to view the Internet headers. Notice who sent this message – dccz@houston.rr.com Software on our email server flags the message with a SPAM-HIGH designation

If the email address looks correct and is familiar, it's most likely legitimate. Internet headers can be spoofed as well though so be aware that this is **only one step to determine if an email is valid**.

If the email address looks suspicious (the **address is cryptic** or has an **international extension** that you aren't expecting – see this month's Tip of the Month), then close the dialog box and delete the message – both from the Inbox as well as the Deleted Items folder.

I Received an Undeliverable Message. What do I do?

If you receive a message like the one below and you don't recognize the email address in the body of the message (skruschw@slip.net), **DELETE** it. In this case, the email was crafted by a spammer and configured to look like an undeliverable message in hopes that you will respond. If you do, they have a live email address (yours) which they can sell for a lot of money.

This is a typical email phishing ploy!

TIP: Look for an address in the body of the email. Do you recognize it (skruschw@slip.net)? If not, delete the email.

```
-----Original Message-----
From: MAILER-DAEMON@mail.firstworld.net
[mailto:MAILER-DAEMON@mail.firstworld.net]
Sent: Tuesday, June 26, 2007 1:13 PM
To: mark@readynetgo.net
Subject: failure notice

Hi. This is the qmail-send program at mail.firstworld.net.
I'm afraid I wasn't able to deliver your message to the following addresses.
This is a permanent error; I've given up. Sorry it didn't work out.

<skruschw@slip.net>:
The users mailfolder is over the allowed quota (size).

--- Below this line is a copy of the message.
Return-Path: <mark@readynetgo.net>
Received: (qmail 24033 invoked from network); 26 Jun 2007 17:12:49 -0000
Received: from unknown (HELO spamninja2.data393.net) ([65.38.161.101])
          (envelope-sender <mark@readynetgo.net>)
          by mail.firstworld.net (qmail-ldap-1.03) with SMTP
          for <skruschw@slip.net>; 26 Jun 2007 17:12:49 -0000
Received: from localhost (localhost.localdomain [127.0.0.1])
        by spamninja2.data393.net (Postfix) with ESMTP id BAD191891E
        for <skruschw@slip.net>; Tue, 26 Jun 2007 11:12:49 -0600 (MDT)
Received: from spamninja2.data393.net ([127.0.0.1])  by localhost
(spamninja2.data393.net [127.0.0.1]) (amavisd-new, port 10024)  with SMTP id 12621-06
for <skruschw@slip.net>;  Tue, 26 Jun 2007 11:12:48 -0600 (MDT)
Received: from 121.246.2.56.dynamic.hyderabad.vsnl.net.in (unknown
[121.246.2.56])
        by spamninja2.data393.net (Postfix) with ESMTP id 8B47B153FA
        for <skruschw@slip.net>; Tue, 26 Jun 2007 11:12:16 -0600 (MDT)
Received: from cdvom ([192.237.253.53])
        by 121.246.2.56.dynamic.hyderabad.vsnl.net.in (8.13.4/8.13.4) with SMTP id
x991746802471i5Aj013429
        for <skruschw@slip.net>; Tue, 26 Jun 2007 22:41:52 +0500 (CDT)
        (envelope-from iaron@familynet.bc.ca)
Message-ID: <02a901c7b815$17aee3b0$3802f679@cdvom>
From: "iaron" <iaron@familynet.bc.ca>
To: <skruschw@slip.net>
Subject: niggardly crank case
Date: Tue, 26 Jun 2007 11:32:05 -0600
```

What is Spoofing / Phishing?

Have you ever received an email with your name in the "From" field? Were you flabbergasted that your name could be associated with SPAM?

Sending email from someone else's address is known as **spoofing**. While SPAM can be clearly recognized, spoofing is much more difficult. Spoofing attempts to trick people into looking at and responding to email by using a recognizable name in the From field. In reality, the email is coming from a person or group that is NOT legitimate.

I received an email with my name (or address) in the From field and I didn't send it. How can this happen?

1) An infected computer (yours or someone else's) sends emails to entries in the computer's address book and randomly puts addresses in the From field (which could include your name). **Example:** A friend's computer is infected with a virus and your name is in their address book. The virus can send an email **to you** and put your name in the **From field as the sender**.

2) A spammer has used special software that modifies the sender field of emails. The From field may show your first name, your full name, your email username, or your email address.

Both of these examples cause a lot of confusion and really throw a wrench in the basic trust that law abiding citizens have with one another. Unfortunately, **there is no way to control who sends messages to whom unless the whole SMTP system is revamped.**

Phishing

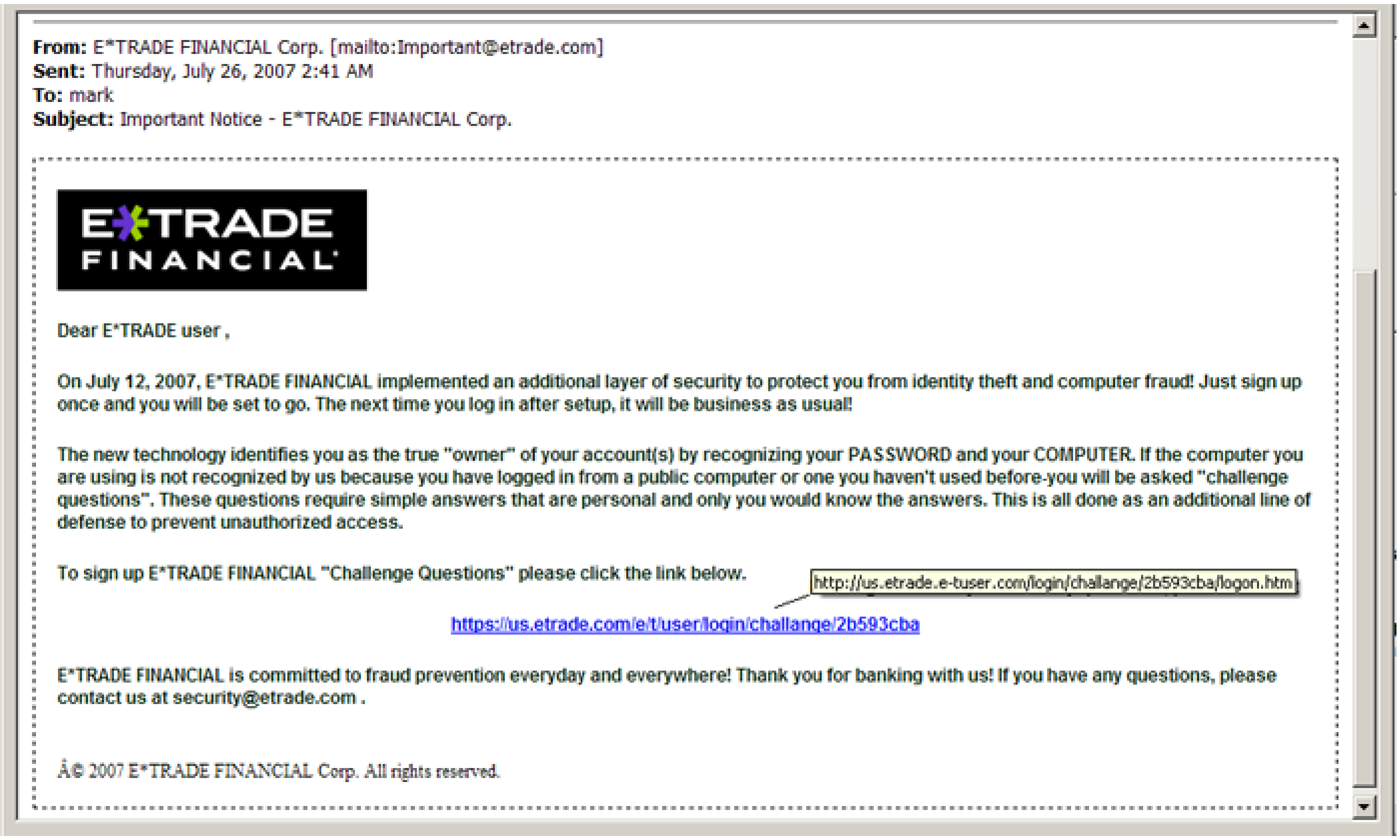
Phishing is a type of spoofing specifically geared to obtaining credit card or financial information from unsuspecting users. While spoofing can involve practices to ruin a company's reputation or cause a loss of revenue from angry customers or lost sales, phishing attempts to defraud people using scare tactics and familiar websites and logos.

An example of phishing would be a message seemingly from your bank stating they will close your account if you don't update your information by clicking a link in the email. After you click the link you're taken to a 3rd party website that looks like your bank's website. You fill in your bank account number and /or social security number and your identity is stolen. It happens everyday to unsuspecting people – BE VIGILANT and learn how to recognize phishing emails. Above all, **DO NOT click links in the body of an email** – type a known address in a browser (e.g., Internet Explorer, Firefox) or use a bookmark instead.

Another tip is to look at the web **address** that appears in the **lower left corner of the browser window** when you mouse over a web link or right click the text and choose Source from the list. Make sure the address is the same in both places and that it looks legitimate. Most false web links will have extra words, IP addresses or multiple extensions showing in the address as in Figure 2.

IMPORTANT: For web links, the text you see on the page or in the body of an email or website is used for reference only. The actual link that is displayed when you roll over it with your mouse is the most important link to look at and be wary of. Whatever address appears when you roll over the link is the page that will open when you click on it. *See Figure 2 on page 5*

Remember: If the two links don't match exactly, don't click on it.



From: E*TRADE FINANCIAL Corp. [mailto:Important@etrade.com]
Sent: Thursday, July 26, 2007 2:41 AM
To: mark
Subject: Important Notice - E*TRADE FINANCIAL Corp.

Dear E*TRADE user ,

On July 12, 2007, E*TRADE FINANCIAL implemented an additional layer of security to protect you from identity theft and computer fraud! Just sign up once and you will be set to go. The next time you log in after setup, it will be business as usual!

The new technology identifies you as the true "owner" of your account(s) by recognizing your PASSWORD and your COMPUTER. If the computer you are using is not recognized by us because you have logged in from a public computer or one you haven't used before-you will be asked "challenge questions". These questions require simple answers that are personal and only you would know the answers. This is all done as an additional line of defense to prevent unauthorized access.

To sign up E*TRADE FINANCIAL "Challenge Questions" please click the link below.

http://us.etrade.e-tuser.com/login/challange/2b593cba/logon.htm

https://us.etrade.com/e/t/user/login/challange/2b593cba

E*TRADE FINANCIAL is committed to fraud prevention everyday and everywhere! Thank you for banking with us! If you have any questions, please contact us at security@etrade.com .

Â© 2007 E*TRADE FINANCIAL Corp. All rights reserved.

Figure 2. Sample phishing email showing mismatched web links

In the example above, the email has the same logo and looks very similar to an actual E*Trade email. Notice the generic greeting and lack of contact information. The biggest giveaway is that the link that appears on the page is different from the one that appears when the mouse rolls over it. Notice the domain goes from https://us.etrade.com to http://us.etrade.e-tuser.com

As subtle as this is, there are two important indicators here: the domain loses its secure designation https: to http: and the domain name is changed to .etrade.e-tuser.com. The "us.etrade" in the false site's domain is a sub-domain of "e-tuser.com" created for the sole purpose of confusing users. The final test was looking at the Internet headers which show that the email did not originate from the .etrade.com domain but from somewhere else.

How to detect a phishing email

1. Look at the URL(s) in the email. Does the text in the link match the text when you rollover it with your mouse? Look in the lower left corner of Outlook and match this text with what's visible in the body of the email. Look closely at the spelling of domain names. It's common for phishers to transpose letters such as http://www.mircosoft.com instead of http://www.microsoft.com

2. Does the email give you multiple ways of contacting the company or MUST you click the link provided? Look for a toll free phone number and verify it against documentation you already have.

3. Are you given a short timeframe to deal with the problem mentioned in the email? Does it state you have 48 hours, 3 days, or 12 hours to respond or else your account will be closed? Most companies will give you time to address issues and will send follow up emails or letters. Phishers will try to feed on people's emotions by establishing a sense of urgency.

GOOD PRACTICE: If you do have a problem with your account, it's best to call someone at the company directly to ensure that the problem is being addressed.

4. Is the email personally addressed to you or is it a generic greeting? Most phishing emails are sent out in bulk so they are usually addressed to "valued customer", "member", etc.

Identity theft has become an enormous problem. Companies realize this and most have changed their policies. Email is cheap, however, and it saves paper so most companies will continue to correspond with their customers via email. You should not be asked to divulge passwords, account numbers or social security numbers via email however. And email messages you receive from your financial and credit card companies should not contain your personal information. If any valid correspondence includes this information, complain immediately.

CONCLUSION

Unfortunately, SPAM and phishing messages will not be going away anytime soon – unless we enact tough laws (i.e., economically detrimental) that are actively and strategically enforced. The best we can do now is to learn to recognize SPAM and phishing emails (look at who is sending the message, the subject and whether there is an attachment – you may need to look at the Internet Headers to confirm it's actually SPAM), use software that aids in filtering out unwanted messages and delete these messages permanently. The more people open and respond to suspicious emails, the more we will receive.

Other safe practices include:

1. Running and regularly updating anti-virus software as well as anti-spyware software.
2. Using a firewall – hardware or software.
3. Downloading the latest updates for your Operating System, Windows XP or Windows Vista, through Windows Updates. **Microsoft releases critical and security updates every Tuesday.**
4. Deleting unnecessary cookies and Temporary Internet Files.
5. Typing the web address directly into a browser address bar instead of clicking a link in an email. It takes a few seconds longer but if the worst happens, it will prevent hours or days of lost time.
6. If you receive a message from your bank or credit card company, is it well written? Are there numerous typos or incomplete sentences? **When in doubt, throw it out** and call the company directly.
7. Don't click on a link if the text that appears on the page is different from the text that appears when you rollover it with your mouse or after checking the source of the link (by right clicking).
8. Look for the lock icon in the lower right corner of the browser window when you should be on a secure site (entering personal data).
9. Don't reply to a SPAM message. **By replying, you are actually setting yourself up for more SPAM**.
10. Lastly, be **vigilant,** be **detail-oriented,** and become **educated** about SPAM, spoofing and phishing.

Phishing Test

Take a phishing test to see how good you are at detecting phishing emails:
http://www.sonicwall.com/phishing/index.html (Hint: some of these are legitimate)