Subject: FW: Seltek Tech Tips E-Newsletter August 2011

SELTEK technology solutions

Seltek Tech Tips August 2011

Seltek welcomes Scott Lints!

Scott joins Seltek as Director of Operations. He brings over 12 years of experience including IS management, IT procurement and sales, logistics and enterprise system administration.
Scott holds a Bachelor of Business Administration degree from Campbell University and a Masters of Science degree in Information Systems from Virginia Commonwealth University.

To learn more about the computer forensics and e-discovery services of Seltek, Inc. go to

Seltek Website

The Windows Taskbar and Quick Launch Bar

Access your programs quickly and easily with this simple Windows trick

If you use Windows 7, you might notice that there is an area for program icons next to the start button. This is known as the taskbar. You can "pin" shortcuts to

Is it Real or is it Spam?

Learn to spot the differences between genuine and junk email
By Kara Mueller, Primary Help Desk Analyst

Most businesses rely on spam filters to determine the legitimacy of incoming e-mail. Yet filtering technology remains far from perfect, and sometimes junk mail might still end up in your inbox. This fact makes it important to be able to visually spot the differences between real email and the digital rubbish spammers generate. Being able to quickly tell the difference between real email and spam will help you save time, unclog your inbox and pay closer attention to the messages that you really want to read.

Finding the Differences

When it comes to spotting spam, here are some things to look for:

Step One: Subject.
Your first action when examining an email should be to check the subject line. Spammers (people or companies trying to sell something) try their best to make their emails look legitimate, yet an email's heading often betrays its true motive. Things like advertisements for herbal medicines and home-equity loans are usually quite easy to spot, since they often have hyperbolic headings like "Incredible Bargain," "Special Report," or "Limited Offer." Phishing messages (which try to steal your personal information) can usually be identified by headings such as "Immediate Action Required" or "Verify Your Account."

Cryptic subject lines, such as "Frank told me to write you" or "Important business question," are more difficult to interpret and will require you to investigate the message more fully. Any messages without a subject should also be checked out more thoroughly, since it may be either spam or a genuinely important letter that was sent in haste.

Step Two: Sender.

your favorite programs, files, or even websites to this area to make them more accessible and help de-clutter your desktop.

To pin a program shortcut to the taskbar, do one of the following:

* If the program is already running, right-click the program's button on the taskbar and click Pin this program to taskbar.

* Or if the program isn't running, click Start, find the program's icon, right-click the icon, and then click Pin to Taskbar.

* You can also pin a program by dragging the program's shortcut from the desktop or Start menu to the taskbar.

In Windows XP, the customizable Quick Launch Bar also gives you convenient shortcuts to your favorite programs, folders, and files. It works much like the taskbar.

* If the Quick Launch Bar isn't already visible to the right of the Start button, you'll need to turn it on. To do that, right-click an open area of the taskbar. Hover your mouse pointer over Toolbars, then click Quick Launch. The Quick Launch Bar appears on your taskbar.

* To add a program shortcut to the Quick Launch Bar, click and drag the shortcut for the application you want to the Quick Launch Bar. Release the mouse button and the application's icon appears in the Quick Launch Bar.

* To remove a shortcut from the Quick Launch Bar, right-click on the icon in the Quick Launch Bar, clickDelete, and then click Yes when asked if you're sure you want to delete the shortcut. Note: Although the shortcut is removed from the Quick Launch Bar, the actual application, folder, or file has not been deleted from your computer.

An email's "from" line can provide significant clues about a message's worthiness. You already know the names of people you regularly correspond with, so it's easy to spot messages from these individuals. On the other hand, emails with a from line that contains only a company name are often spam or phishing lures. To research any message's legitimacy, check out the email's return path to verify that it leads back to the person or organization that it purports to come from.

The trickiest emails to decipher are the ones sent by total strangers, who may be spammers or individuals posing a genuine business question or offer. The only method of determining the legitimacy of these messages is to investigate still further.

Unfortunately, some spammers are able to "spoof" e-mail addresses, meaning the e-mail will appear to be sent from somebody you regularly correspond with, somebody in your office, or even yourself. The subject line and body will often contain the advertisement or sometimes a single link. If you are unsure of the contents of the e-mail, contact and confirm with the sender if they have indeed sent the e-mail.

Step Three: Dates.
The dates can sometimes provide a clue to an email's value, and take less than a second to check. If a message with a far past or future date suddenly arrives, it's more than likely from a spammer seeking attention.

Step Four: Content.
If you're still not sure about a particular message's authenticity, examine its content. If an email addresses you as a "friend," "valued customer," or "colleague," it's likely the sender doesn't know your name.

Poor grammar, bad spelling and awkward, non-native use of English are other signs that should arouse your attention.

Be on the lookout for Web links that lead to suspicious sites (such as a message from someone supposedly at Amazon.com that contains a link leading to a non-Amazon site). Do not click on a link you don't trust. To find out where a link will take you without opening it, hover your mouse cursor over the link to see the real address it will take you to. Examine this address closely! Con artists also often use URLs that resemble the name of a well-known company but are slightly altered by adding, omitting or transposing letters. Remember that legitimate websites (such as shopping or banking sites) will never ask you to send your password!

Step Five: Attachments.
Never open an attachment unless you know who sent it, or at least understand why it was sent to you.

The Bottom Line:
Knowing how to tell the difference between real email and spam will help you save time and potentially

For more information about any of these topics, contact the Seltek Help Desk at (804) 360-4490 x7 or e-mail us.

spare you from financial, professional and emotional loss.

Contact Seltek at 360-4490 to set up a review of your processes!

Seltek Featured in Henrico Citizen

The Henrico Citizen newspaper featured Seltek's people and services in its issue last week.

"Seltek has dealt with cases involving theft, counterfeit, copyright, fraud, breach of contract, bankruptcy, and wrongful dismissal, among a few. The computer forensics division of Seltek serves clients nationally and is one of the only companies in Central Virginia that provides both IT support and computer forensics services."

To read more, click here for the article online "Technology Police"

Forward email

SafeUnsubscribe

Trusted Email from Constant Contact FREE
Try it FREE today.

This email was sent to carole@cytconsulting.com by wendy@seltekinc.com |
Update Profile/Email Address | Instant removal with SafeUnsubscribe™ | Privacy Policy.
Seltek | 8814 Fargo Road | Suite 105 | Richmond | VA | 23229