10-1-2006

Digital Hygiene: Email Techniques

Charles Boulet
Pacific University

Follow this and additional works at: http://commons.pacificu.edu/inter06

Recommended Citation

This Article is brought to you for free and open access by the Interface: The Journal of Education, Community and Values at CommonKnowledge. It has been accepted for inclusion in Volume 6 (2006) by an authorized administrator of CommonKnowledge. For more information, please contact CommonKnowledge@pacificu.edu.
Digital Hygiene: Email Techniques

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter06/37
Digital Hygiene: Email Techniques

Posted on November 1, 2006 by Editor

By Charles Boulet <charles@pacificu.edu>

If you read no further, go to the End Notes of this article and click on the links for additional information about Identity Theft and how to protect your resources.

No apologies are offered for once again focusing on Microsoft in an article on security. Outlook, Outlook Express, and Exchange servers are the training grounds for new hackers, phishers in particular.

It is of no small consequence nor coincidence that the simple acronym ‘IT’ represents both “Information Technology” and “Identity Theft”. In previous epochs, identity theft was relatively rare, globally condemned, and harshly punished. In a new age of information technology, the cost of identity theft is counted in the billions annually in the U.S. alone, and the perpetrators often exist as ghosts, never to be found, never brought to justice. The true and total cost to society of identity fraud is, of course, incalculable; a simple search reveals endless tales of real people, victims, completely financially ruined because of the loss of control of their credentials.

Wikipedia tells us: “In computing, phishing is a criminal activity using social engineering techniques. Phishers attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message, although phone contact has been used as well. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, and technical measures.”

In the previous article, software was described that should eliminate nearly all of your risk of exposure to phishing and other traps. Even if used correctly, however, well-crafted software can save the user from many things, but it can never guarantee protection from the user himself. This article focuses specifically on email usage and etiquette with a view towards inculcating a strict code of behavior. This ‘email code of conduct’ is guaranteed to eliminate a large part of the remaining risks to your most private data and financial resources.
Changing Behaviors

It is not a difficult thing: Open Outlook, Press the F1 key and search for “Junk Mail Filter” and “Rules and Alerts”. Undertaking this simple task will lead you instantly to everything you need to know about filtering your incoming mail so that you no longer have to deal with the unwanted annoyances: Small things such as the loss of time, data, and money.

But no, wait, in just a minute or two, after you finish downloading that next morsel from YouTube. It’s a great clip, you know the one: The monkey in the tree, scratching itself, then falling off the branch. I laugh every time I see it.

In procrastinating in matters of security, you agree to an implicit arrangement whereby you trade off potentially hundreds, even thousands of hours of work as lost data, and even more financially, in exchange for little to nothing of value. If you refuse to take measures to protect yourself, be prepared for the worst to happen; even then, when the worst comes you may no longer have the resources to deal with it. And never forget that very often you are not the only victim when your identity is ‘borrowed’. Our own email habits have direct impact on those people who receive the emails we send out. Often, unwittingly, we openly share severe threats between friends and business colleagues. Sorry hardly begins to suffice.

If, having read this last paragraph, you feel a little sheepish, relax. If you have not started using junk mail filters, breathe easy. After reading this article, press F1 and get to it. In computing, especially in the home or small office, a little bit of effort can frequently lead to great, though sometimes invisible, rewards. There are no bells or flashing lights when a system is protected, and so it is not typically exciting. But in the quiet, our protective measures seamlessly integrated into our computing life speed us along and make us more efficient, save us hours of technical troubleshooting, spare us the stress and grief associated with screening unwanted mail, and keep our bank accounts in order.

The core steps required in protecting yourself are simple for the most part and are presented below. Be forewarned and prepared in dealing with advanced features of your favorite email client: Be patient with the software and with yourself and press F1 whenever you would like some help. Copy/Paste the following checklist into a new word processing document and print it to create a guide to keep by your keyboard. Perhaps you have other ideas that you would like to add. Glance over it occasionally to review the steps left undone and ask yourself why not protecting your information is a better idea than protecting it.

Here is the check list. More detail regarding each item is provided below.

1. “F1”. Say it again, “F1”.
2. Avoid Suppression
3. Organize your inbox and throw out your trash.
4. Scan incoming mail (and all IM conversations).
5. Use Junk Mail filters.
6. Use Rules and Alerts.
7. Always verify Net address before clicking on an email link.
8. Save attachments and scan them prior to opening.
9. Scan outgoing mail.
10. Decide between BCC, To, and CC.
11. Clean mail before FWD.
12. Use Plain Text if possible.
13. Send other doc formats as attachments.
14. Send attachments as .zip or .rar files.

1. “F1” is the standard call for HELP in Windows software.

2. **Avoid Suppression**: Our brains tell our vision to stop considering information we do not want or no longer need. It streamlines visual information processing, but it also helps us to ignore obvious answers that lie before us. Standard menus and ‘pop-up’ (right-click) menus contain smart and useful features that remain unused for the most part. Open your eyes to the various options that appear along with your favorite items. Also, try right-clicking on objects (folders, email items, and most everything else, including menus themselves) and you will open up a new world of powerful new tricks.

3. **Inbox**: Organize your inbox and throw out your trash. Create folders and subfolders to organize items you wish to keep. Also, users typically save more information than they need in the Sent Items or Deleted Items folders, for example – old data that is never referenced. Anything of doubtful value or origin should be purged. Always remember to purge the Deleted Items folder (right-click the folder for the option to empty it).

4. **Scan incoming mail**: Set your antivirus software to scan all of your incoming mail for all threats. New tools will also cover instant messaging streams.

5. **Use Junk Mail filters**: Set filters to recognize junk mail and then direct it to either the Junk Mail folder or the Deleted Items folder. Outlook has a ‘Blocked Senders’ list. To add a mail to the list, right-click the item, select Junk E-Mail > Add Sender To Blocked Senders List.

6. **Rules and Alerts**: Many email clients offer the ability to create rules that are applied to incoming items. As an example, upon receiving an item from UncleBob@MyFamily.com, your rule might send the email from UncleBob to the “Family” folder you created, and then play a sound to tell you that it was there. Perhaps a more pertinent example is a new rule that flags any incoming mail from a doubtful source, say ‘FalseName@YouveBeenHacked.com’ and any other mail from the ‘@YouveBeenHacked.com’ domain and simply delete it. Create new Rules then run them immediately to test them.

7. **Always verify Net address before clicking on a web link in an email**. Hold your cursor / pointer over this link: www.YoureAWinner.com. You will most likely see the actual address of the link you are intending to click, either as a popup message or in the status bar at the bottom of your web browser. (No need to click, but feel free to try.) A link is rarely what its text would suggest. The next article in this series will address the issue of
misleading links and other traps one often finds while living in a connected world.

8. **Save attachments and scan them prior to opening.** This is the best practice, but once you get to know your own data you can forego scanning trusted material. Try creating a temporary folder “Mail Temp” on your desktop; you can drag your attachments from the mail message to the Mail Temp folder and scan the items from there before you open them. Your antivirus software might already be set to scan your mail attachments automatically as they are received, and so to scan the attachments again would be redundant.

9. **Outgoing mail scan.** The best way to avoid infection is to not spread one. Again, set your antivirus software to scan all mail that leaves your computer – this will catch all the mail you send deliberately and any other messages that are sent without your knowledge.

10. **BCC vs. To vs CC:** Always deliberately choose how your email is addressed and be aware of who sees the addresses on your sent emails. It seems obvious, but improper addressing in email is the leading way hackers obtain current valid email addresses.

   A. **To:** All recipients of an email address will see addressee names listed in the To list.

   B. **CC:** (Carbon Copy). Addressees listed in the ‘CC’ list of an email are also visible to all recipients. The ‘CC’ designation is functionally equivalent to ‘To’, and so the difference is in protocol and intent; you include someone in the ‘CC’ to simply make them aware of a communication with your primary recipients (‘To’) or to make the primary recipient aware of the copy to those listed in ‘CC’.

   C. **BCC:** (Blind Carbon Copy): Addressees listed in the ‘BCC’ list see names of all recipients in ‘To’ and ‘CC’ lists, but the BCC names themselves are invisible, hence ‘To’ and ‘CC’ recipients are ‘blind’ to the fact that ‘BCC’ addresses will also receive a copy of the email. Security-minded users will often add all addresses to the ‘BCC’ list and add either no addresses at all to the ‘To’ and ‘CC’ lists, or simply add their own address to the ‘To’ list. This way, recipients see that the sender is on the list (presumably a safe sender), but they are the only other recipient; even if the mail is sent to dozens or hundreds of addresses, the individual recipients will only ever be able to glean their own address and the sender’s address from the email.

11. **Clean mail before FWD.** We often forward mail we receive to other new recipients with whom we wish to share the information. Take for example a message received from someone who received it from someone else who in turn received it from another source, and so forth; like moss, new addresses and user names accumulate on the forwarded message with each new send. In forwarding this message, we are sending, along with the relevant content in the email, other email addresses and names of recipients who had received the mail before us. This is an easy way for hackers to collect active valid email addresses of potential victims. Remember to strip all unnecessary information from your emails before forwarding them on to others, especially others’ personal information.

12. **Use Plain Text if possible.** While lacking in flair and expressive potential, plain text email is much more secure and free of potential threats than is ‘rich text’ email or HTML mail messages. Formats in order of increasing risk are: Plain Text, Rich Text, MS Word / HTML.

13. **Send other document formats as attachments;** that is, if you need to send pictures, formatted text, movies, or anything that plain text will not support, nothing is safer than to
send it as a separate file. If you must include formatted text and a picture, for example, create a word processing document and send it as an attachment.

14. **Send attachments as .zip or .rar files.** When you compress a file into a .zip or .rar format (other formats exist as well), you place an additional layer of protection between your system and the attachment while gaining the added benefit of sending a file of reduced size, which saves time in the sending process. A compressed file must be extracted (decompressed) before it can be executed, so you must be very deliberate in opening the file and this can give you a second chance to scan the contents. Conversely, should you decide to send a file that Outlook might find threatening (such as a simple web link/URL), you can first compress it (‘zip it up’) before sending; from Outlook’s perspective, you are simply sending a .zip file, and not a potential threat (.htm or .lnk file).

15. **Use Simple Link Names.** If your mail includes a link to a resource on the Internet, including any web page, media link, or any other link external to the local network, be certain the link text is the same as the actual address. For example, if you would like to send a link to a friend for [www.microsoft.com](http://www.microsoft.com), make the link text the same as the actual address, rather than having the text say “MS” with the underlying URL as [www.microsoft.com](http://www.microsoft.com).

**Notes:**

Read the Attorney General’s advice regarding identity theft:

Additional ‘IT’ resources:
http://www.consumer.gov/idtheft/
Search for identity theft insurance and other solutions here.

Living in the IT Age has many benefits, not the least of which is that the Age itself is so well documented. Refer to [http://en.wikipedia.org/wiki/Phishing](http://en.wikipedia.org/wiki/Phishing) for a great historical on phishing.

This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=3306].