Thoughts on email - a technical exploration

The objective of this paper is to explore ways to improve the effectiveness and safety-from-hackers of email communication.

I will go into some technical details, but not real deep. Just enough, I hope, to aid understanding of how things work and why you might choose one option over another.

Email Clients

When you compose an email, you are running a program ('app' or 'application') called an email client. There are many email clients available, but the most common are:

Mail - by Apple, for Mac OS and iOS
Outlook - by Microsoft
Thunderbird - by Mozilla

The Wikipedia page http://en.wikipedia.org/wiki/Comparison_of_email_clients lists over 60!

You use the same email client for creating, receiving, reading, deleting, replying to emails that you get.

When you compose your email, you can create it in one of two ways:

Plain text - single font, no formatting, no highlighting, no colors, *etc*.

Marked up text - mix font faces, font size, font weight (normal, bold, italic ...), colors, *etc*.

When you use marked up text, you actually don't see the mark up: your email client renders the text using the fonts and effects you want. Behind the scenes / under the covers the email client is marking up the text in a way that communicates your desired effects to the email client of the person you are sending the email to when they read it.

Similarly, when you receive an email you have a choice (typically under Options, Settings, Tools, or some such menu item) to display just the text of an email or to the have the text rendered as the sender marked it up. So you see the same fonts, colors, highlighting, etc. as the person who wrote and sent you the email.

But beware: someone can send you an email that contains malicious markup: when your email client tries to format / render the text, the markup might actually contain hidden software commands that can get control of your client!

However, that's not too common. More of a problem are links and attachments.

Links and Trusting the Sender of an email

Even plain text emails can contain links: the address of a web page, set up so that if you click on the link your web browser is invoked and the specified page is loaded into your browser. A typical link might look like this:

http://trainersfriend.com/takayama/

As most of you probably know, you should never click on a link in an email unless you know and trust the sender! In this case, you get what you deserve.

How do you know you know the sender?

Look at the header display

* the 'From' might not even be someone you know

* the 'From' might be a name you know but it is followed by an email address in angle brackets, such as:

Steve Comstock <jerry@trouble.com>

Although this email is ostensibly from me, the real 'From' address is the value in the brackets, that is 'jerry@trouble.com'

* the same comments apply for a 'Reply to' header if shown

Finally, even if the sender seems to be someone you know and trust, the from or return addresses can be 'spoofed' - made to look like someone you know. In that case, your best defense is judgement: is the topic or tone of the email in character with the person you know?

Attachments

Everyone likes to attach a file to an email from time to time. A document (Word document, PDF file), an image (logo or snapshot) or mp3 (music) file, etc. Different email clients handle attachments differently.

But beware: when you open an email with attachments, some email clients render the attachments as if they were in the email itself. Other email clients just show you the names of the attached files and give you a choice to save the file or open it using a separate app (such as Adobe PDF Reader or Windows Photo Viewer).

The most dangerous are the email clients that embed attachments when they render the file! That is, the attached PDF document displays in the body of the email, or the Word document is displayed in all its glory. This is dangerous because there are so many more places to hide malicious code in the rendering tools that convert the internal formats of Word or PDF or image files.

Email Security

So, the safest way to view email is to have it rendered as plain text and set up so that attachements just show as file names instead of being embedded in the email as you look at it.

> Boring!
>
> Yup, but safe.

It's also good to have a security client that will scan email attachments for known malicious software and that will also warn you if a link is to a suspected site.

My Approach

I compose all my emails as plain text.

The email client I use is called Thunderbird, it's free, from Mozilla software. Under the 'Tools' menu is a choice called 'Account Settings'. This has a list of choices including one called 'Composition and Addressing'; this is a dialog box with the first line being a check box labeled 'Compose messages in HTML format' - if I check this box I will be using marked up text. I make sure this box is not checked.

Also under 'Tools' is a choice 'Options' which has several tabs for setting values. On the 'Display' tab I choose my default font as Courier New 14 point.

> Generally speaking, I prefer monospaced fonts over variable width fonts. With a monospaced font it's easier to line up columns when it's important to have consistency in data in columns: each character takes up the same width. The font this paper is written in is 'Arial', and that is a variable width font. Notice, for example, that in 'Generally' that the 'G' takes up much more space than the 'l's. The Wikipedia page
>
> > http://en.wikipedia.org/wiki/Samples_of_monospaced_typefaces
>
> displays samples of several monospaced fonts

Staying with the 'Options' choice under 'Tools', look at the 'Privacy' tab; uncheck the box labeled 'Allow remote content in messages'. On the same tab I check 'Accept cookies from site' along with 'Keep until:' set to 'I close Thunderbird'; cookies can be useful / helpful, but no need to keep them around after your email session is done. In the same place is a button labeled 'Tell sites that i do not want to be tracked'. I check that. It's an honor system, but I believe it keeps some companies from tracking my references to their sites.

There is an add-on (also free) to Thunderbird called Show HTML that allows me to display marked up text formatted as the sender desired. When I know an email is from someone trusted, I can click on the 'Show HTML' menu choice and I will see the fully rendered email - so the ability to read marked up text as intended is fully under my control.

How to add some formatting with plain text

There are several techniques I use to make my plain text emails have a little pizzazz to them:

* I keep lines short; that is, I press <Enter> to start a new line after only
65-80 characters (actually, an ending 'space' then<Enter>).

> The purpose of this is to avoid 'word salad': strings of letters
> so long you have to scroll to read the email. Keep the eye
> movement short
>
> One problem with this is: some email clients run them together
> anyway, defeating my attempts to create some visual blocks

* I add an extra blank line between paragraphs (putting a blank on each line);
again, this is to provide some visual break between ideas

(For those of you who compose email on your smartphone, the above techniques would make your emails more readable for us plain text folks!)

* Sometimes I highlight by drawing arrows:

```
==> Tonight is the big night!
==> Be sure to be there!
```

or what's called a 'flowerbox':

```
*********************************
*                               *
* Here is a flowerbox using  *
* 'Arial' font                   *
* Notice how hard it is to       *
* get the right edge to line    *
* up. This is because of the  *
* variable width font.          *
*                               *
**********************************
```

```
*****************************
*                           *
* Here is a flowerbox using *
* 'Courier New' font.       *
* Notice how nicely the     *
* right edge lines up.      *
* This is because of the    *
* fixed width font.         *
*                           *
*****************************
```

There are three other techniques available with plain text:

If you surround a text string with _ (underscores), the text will be underlined. So if you key in

This is _very important_

it will display as

This is _very important_

If you surround a string with * (asterisks) the text will display as bold. So

I want *you* to help me out

will display as

I want __*you*__ to help me out

If you surround a string with / (forward slash), the text will show as italic. So

This campaign is /very important/

will display as

This campaign is */very important/*

Thoughts on Content: making emails more effective

I have found that shorter emails are most effective.

People don't take the trouble to read the whole email if it's longer than two or three paragraphs. For me, I'm just getting going with that.

Generally cover only one topic in an email.

Bullets are often more effective than text.

If you have to write a really long email, put a bullet summary at the top (in the same order as your topic points). I also find separator lines between topics help emphasize the break.