Sussex County Public Schools

Technology Training Guide - E-MAIL Best Practices

General

- NEVER, EVER, NOT EVEN ONCE Send Credit Card, Bank Account, or Passwords details, via email. Emails are often sent as plain text and are not encrypted meaning that it is possible for people to intercept and read email traffic.

- NEVER, EVER, NOT EVEN ONCE configure Outlook Web Access [OWA] or your browser to automatically remember your password.

- BEWARE of attachments, even if you know the sender. They could carry a virus that is unknown to the sender. Save them somewhere and run antivirus software on them BEFORE opening.

- Do not send large files over email as attachments. Email servers are configured for small file sizes and large attachments can cause large delays to email servers. Please zip large files to transfer, or consider using Google Drive.

- When sending documents via email, remember that not everyone has the same Word processor as you and may not be able to read your document. Save as Rich Text Format (RTF) to avoid such problems.

Spam Emails

Spam emails are typically sent to your address from people that you do not know and contain information you did not request. Basically electronic “Junk Mail”.

If you do not recognize the sender, or if ANYTHING seems "suspicious" (Like the subject line, or the topic) DELETE IMMEDIATELY.

SCPS Technology Department blocks spam/junk emails wherever possible, however due to the nature of the Internet some spam mail will always seep through.

It is recommended that spam mail is deleted. Never reply to spam mail as this only shows the sender that they have a valid mail address.

Offensive Emails

If you receive an offensive email please print it out and turn it in to the Technology Department - Please print the message unedited so that we can trace the origin of the email. Do not delete it from your mail box, as we may need to use it for tracking. Do not reply to offensive mails.

Hoax Emails

There are a number of common hoaxes that are sent via email, including money transfers from overseas, pyramid sales, etc. Please delete these mails and do not reply.

How to handle e-mail attachments

E-mail attachments are a tricky business. They are a necessary and useful tool for transmitting files, yet they are also a high risk security vulnerability. Once opened, an e-mail attachment containing the latest and greatest in malicious code could possibly execute on your system. However, since IT scans incoming and outgoing e-mails for viruses, it is unlikely that an e-mail sent to your Sussex e-mail account would infect your computer. Unfortunately, even the most up to date anti-viruses are not fool-proof, and it is still possible for new and undocumented viruses to pass through our virus scans undetected. In such an event, it is important for you, the end user, to be aware of the threats posed by e-mail attachments and how to protect yourself from opening an unpleasant surprise.

Didn't expect? Reject!

Perhaps one of the most effective ways to prevent opening a virus infected attachment is to not open *any* attachments you did not expect to receive. It does not matter if the e-mail is from a good friend or a reputable contact, if you did not receive prior notification that an attachment was to be sent to you, it may be dangerous to open. Also be careful of messages that contain a generic text greeting. Contact the person who sent you the attachment to confirm that it was purposely sent. If your contact's computer has been infected with a virus, the virus may have been programmed to send itself to everyone on your contact's address book.

Be mindful of file extensions

Make sure to check the file extension of attachments before opening or executing them. Since Windows does not show known file extensions by default, you may need to change your folder options. To view file extensions:

1. Double click on **My Computer**.
2. Select the **Tools** menu and select **Folder Options...**
3. Click on the **View** tab.
4. Uncheck the box beside **Hide extensions for known file types**.

As it would be difficult to create a comprehensive list of all known dangerous file extensions, one will not be attempted here. Instead, be wary of any file extensions you are not familiar with and exercise caution for those you know are capable of running scripts or macros.