Email

How To Spot Dangerous Emails

When you are using your school provided email, every email is scanned before it reaches your inbox. Unfortunately some malicious emails can still get through even the best of scanners. If you take a few minutes and really look at the email, you can often see it is a hoax. And many times, the clues are obvious, if you just remember to look for them. You would be surprised how many people, after they have been infected, say "I thought something about it was off".

- **Does the "From" make sense?** Although the from field can be faked, it is often one of of the easiest ways to check for dangerous emails. Since it can be faked, do not rely simply on this test. (In fact, you should never relay on just one of these to consider the email "safe")
    - Check if the email address makes sense. If the subject is about PAVCS but the from address is a different domain such as "bob@anyotherdomain.com" it is most likely a hoax.
    - Check the email address vs. the name. If you get an email from "jdoe@pavcs.us" and the name shows as "Bob Smith" then it is most likely a hoax.
    - Even when the "FROM" is a friend's email address you recognize, it could have been spoofed. Again, use context clues. Does the email seem like something your friend would send? If it seems suspicious, contact that friend to verify the email (Do not just hit reply, you may be replying back to the hoaxer)
- **Does the "To" make sense?** Many times the sender only has an email address, not your real name. So if you see the email address really is your email address, but the name that shows is not yours, this could be hoax. Sometimes there will be no "TO" or the TO will be someone you don't know, and your email address is in the CC or BBC fields. This could be a clue that the email is a hoax.
- **Does the "Subject" make sense?** Often a hoaxer will use a subject line that will grab your attention. But even these should be suspicious.
    - If it says something about "your recent purchase" and you don't give out this email account for purchases, you should be suspicious.
    - If it doesn't match up with the the sender, you should be suspicious. For example, the subject might be "Your Math Test" but the sender is not your teacher.
    - If the subject has attention getting characters, for example "*****YOU MUST SEE THIS!!!****"
    - Check that the subject line matches with the body. If they don't seem to match, good chance this is a hoax email.
- **Does the "Body" make sense?**
    - One common clue is a number of mis-spelled words and/or improperly used words such as 'there' and 'their'.
    - Is the tone of the email 'off'. For example an email that looks like it is from a friend of yours that you speak with often, but the email feels formal with "Dear NAME," and "Sincerely, YOUR FRIEND". Or maybe the email shows as from your teacher, but the message uses a lot of slang terms.
    - If the email talks about the package you shipped, but you have not

shipped anything.

- **Does it have an Attachment?** May times the hoaxer will try to get you to run some harmful code by using an attachment. If you receive an email with an attachment, use extreme caution before opening it.
    - Were you expecting an email with an attachment? If you were not expecting it, don't open it. Check with the person who sent it before opening it.
    - If the email is from a business/company, don't download/open it. A legitimate business will never ask you to open a file attached to an email.
- **Be cautious of any Links** You should use extreme caution if the email has any links. Never ever click on a link in an email.
    - You should inspect the destination address before clicking on any links. Many email applications let you hover over the link to see the address. If that does not work, you can right-click and choose "copy link" then past that link somewhere safe such as notepad.
    - Does the link make sense in the email? If the email is about your class work, but the link does not go to a school site, then it is probably a hoax.

With just a tiny bit of caution, and "trusting your gut", you can often spot the fake emails from the real one. But should you be unsure, you should always play it safe. Call the sender of the email, or start a new email and ask the sender if they really sent it (do not hit reply).

Unique solution ID: #1047
Author: Kevin Squire
Last update: 2017-05-04 09:37