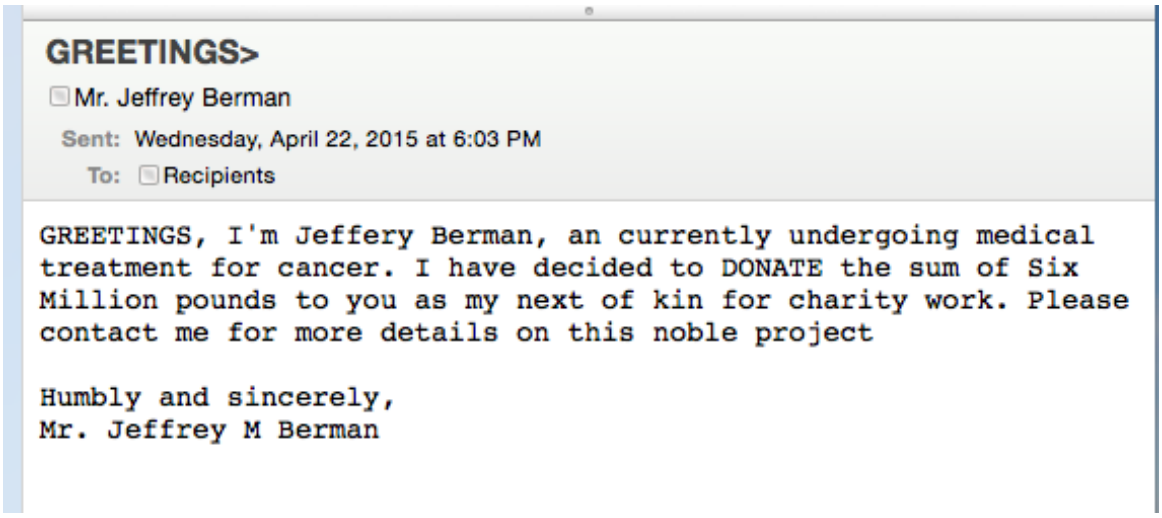
Spam (Junk email and Phishing email) and Pharming (fake websites)

Spam, phishing and pharming are all terms relating to dubious online practices, either to sale goods or services online or to gain access to confidential information, often with malicious intent.

Spam is the term used to describe unwanted (junk) emails that are typically distributed in bulk. Spam messages will typically contain commercial content – examples include pornography, pharmaceuticals, dubious financial transactions, or 'too good to be true' offers. In most cases, spam emails are sent with fraudulent intent, but there are also cases where reputable companies or private users send mass emails too.

An example of Junk email: (to many recipients, requesting a response)



GREETINGS>

Mr. Jeffrey Berman

Sent: Wednesday, April 22, 2015 at 6:03 PM

To: Recipients

GREETINGS, I'm Jeffery Berman, an currently undergoing medical treatment for cancer. I have decided to DONATE the sum of Six Million pounds to you as my next of kin for charity work. Please contact me for more details on this noble project

Humbly and sincerely,
Mr. Jeffrey M Berman

Spam can also be used to launch phishing attacks where users are sent emails tricking them into 'updating' their personal details online via a fake website (imitating a bank or similar). The tricky part is that phishers pretend to be someone you know, like a bank or even a department from right here at Purdue, to make you think they are trustworthy. That's why it's so important to keep in mind that CLA-IT or any other Purdue department will NEVER, under any circumstance, ask you for your login information via email or web form. Anyone asking for this type of information via email is undoubtedly a fraud. Spam can also be used as a means of distributing malicious software, which can install key-logging software on your PC without your knowledge.

Pharming is the term used to describe the process of redirecting users to a fraudulent copy of a legitimate website, again with the aim of stealing personal data and passwords for criminal intent. The definition of pharming might also be extended to include targeted advertising or the 'pushing' of people towards products and services, for example : "people who have bought 'x' have also bought 'y'… and if you do, you will save 10 dollars."

It is also increasingly common to receive SMS spam on mobile phones. A related term – spim – is used to describe spam attacks using instant messaging services. Facebook and other social networking spam is now also very common.

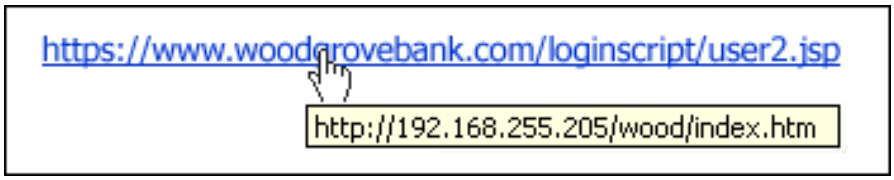
What does a phishing email message look like?

Here is an example of what a phishing scam in an email message:

Keep in mind 4 common traits:

1. Threats
2. Links
3. Popular Company
4. Spelling

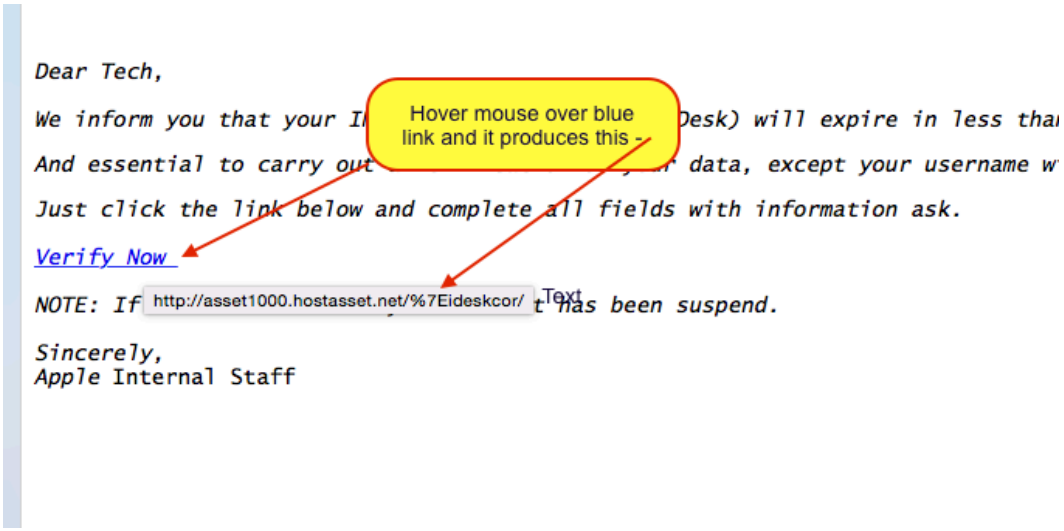
- **Spelling and bad grammar.** Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have a staff of copy editors that will not allow a mass email like this to go out to its users. If you notice mistakes in an email, it might be a scam.
- **Beware of links in email.** If you see a link in a suspicious email message, don't click on it. Rest your mouse (but don't click) on the link to see if the address matches the link that was typed in the message. In the example below the link reveals the real web address, as shown in the box with the yellow background. The string of cryptic numbers looks nothing like the company's web address.



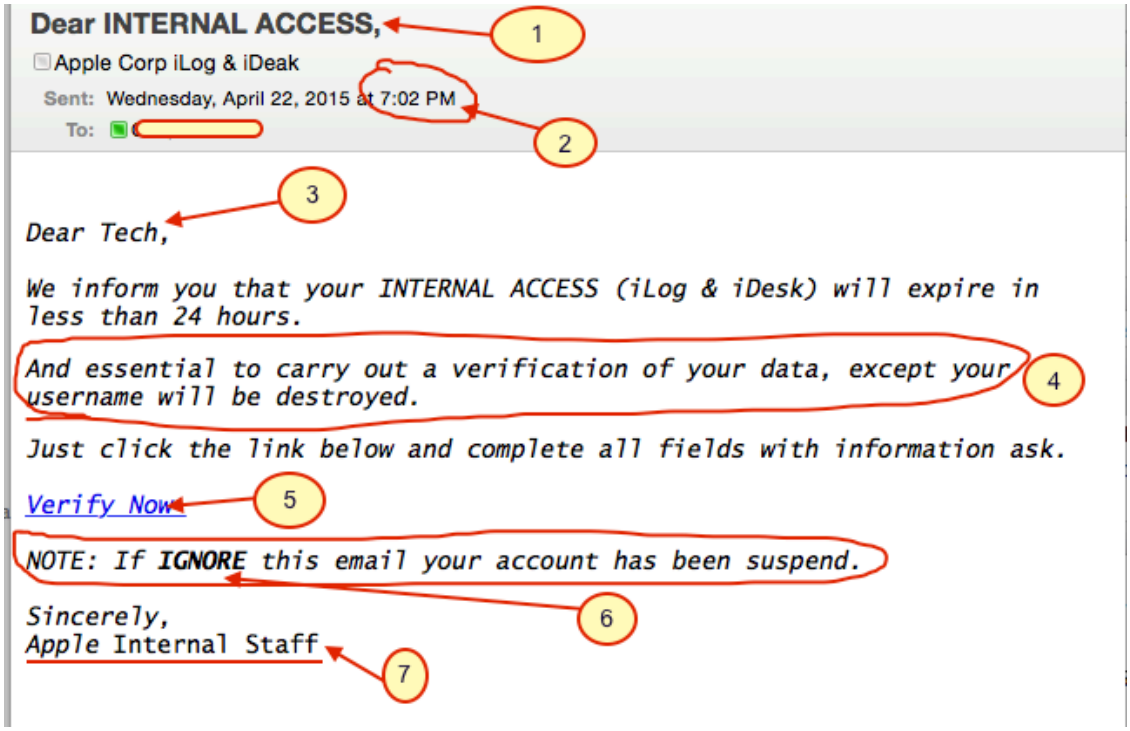
Links might also lead you to .exe files. These kinds of file are known to spread malicious software.

- **Threats.** Have you ever received a threat that your account would be closed if you didn't respond to an email message? The email message shown above is an example of the same trick. Cybercriminals often use threats that your security has been compromised.
- **Spoofing popular websites or companies.** Scam artists use graphics in email that appear to be connected to legitimate websites but actually take you to phony scam sites or legitimate-looking pop-up windows. Cybercriminals also use web addresses that resemble the names of well-known companies but are slightly altered.

Can you spot 7 reasons why this next clip of an email is a Phishing email?
(Remember even 1 reason is enough to trash it!)



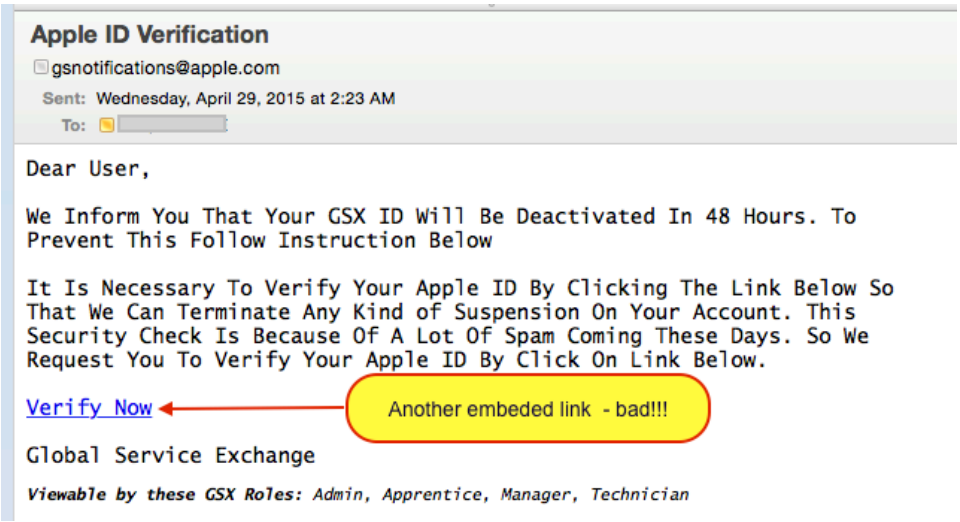
Next picture shows the 7-circled reasons why you should trash this form of an email when you see it:



Explanation of each one:

1. Not addressed to you directly
2. Late at night when most phishing scams occur
3. Not my name, twice addressed wrong and differently
4. Fragmented sentence, as well as the next sentence, neither are grammar correct
5. Embeded link with hidden url (hover over with mouse to see link)
6. Here's your THREAT! (bad grammar here too)
7. Signed by who? (Where is Name, address, & phone #)

Another one from Apple (GSX):



Check out the time on this one – in the AM….

Okay, that covers what it is and how they look, but you need more info. So Ask Questions!

Use your head

Try to encourage all family members to follow this simple routine when using email:

- The **Know** test: Is the email from someone that you know?
- The **Received** test: Have you received email from this sender before?
- The **Expect** test: Were you expecting email with an attachment from this sender?
- The **Sense** test: Does email from the sender with the contents as described in the subject line and the name of the attachment(s) make sense?
- The **Virus** test: Does this email contain a virus? Always check it using anti-virus software.

Don't respond!

If you do receive spam, it is important to never respond even if an **'unsubscribe'** link is provided. By responding, you are alerting the spammer that yours is a valid email address, and this will just increase the likelihood of you receiving yet more spam in the future.

Here are more things to look for when determining if the e-mail you received is legitimate:

- Did the e-mail come to you unsolicited?

- Is the sender a stranger to you?
- Does the e-mail claim to be from a help desk and talk about account "quotas"?
- Does the e-mail claim to be from a help desk and talk about infections?
- Does the e-mail claim to be from a law enforcement agency?
- Is the e-mail from an online shopping site you never use or haven't used lately?
- Does the "To:" field in the e-mail list hundreds of names and e-mail addresses?
- Does the e-mail sound threatening in any way, especially legally or financially?
- Does the sender of the e-mail use poor grammar?
- Does the link go to (example) "purdue.WEBS.COM"? (not purdue.EDU)
- Does the link say, "pUrdue.com" instead of purdue.edu?
- Is the e-mail from an individual's e-mail address instead of an official account?
- Is it tax season?
- Is it a holiday season?
- Has there been a major tragedy in the news lately?
- Did you receive the e-mail early in the morning or late at night (after hours)?

If you can answer yes to any one (or more) of these questions, the e-mail may be a phishing attempt.

Hopefully this gives you enough reason’s to trash any email that comes in unfamiliar or not asked for.