Phishing Email FAQ

What is ‘phishing’?
Phishing (pronounced ‘fishing’) is when a person (the 'phisher') tries to trick you into doing something unwise by sending you a fraudulent email (the 'phish'). Typically, the phish says that your email account will be deleted unless you go to a website where you are asked to type in your email username and password. In some cases, you are directed to a website where you are told to install software on your machine.

Who should be concerned about phishing?
Anyone who uses the University’s information resources (e.g., email, Banner, Blackboard) or who uses a University workstation or who logs into the University remotely. In other words, everyone.

Why should we be concerned about phishing?
Despite its goofy name, phishing is a serious threat to the security of the University, and users who respond to phishing emails are putting the University at significant risk for data breaches, compromised accounts, and public embarrassment. All University computer users are required to educate themselves about phishing. Users who respond to phishing emails can be subject to a range of disciplinary actions, from temporary loss of computer privileges to termination from the University.

Why does the phisher want my username and password?
Typically, to log into your email account and use your email account to broadcast thousands of spam messages. Also, the phisher might use your username and password to masquerade as you and trick other people in the University into disclosing their usernames and passwords. Some phishes install malware on your machine so that the phisher can compromise your machine and other machines on the network.

So the phisher gets my username and password. Why is that such a big threat to the University?
If the phisher sends enough spam from your mailbox, other major Internet mail systems will stop accepting all email from your email address (aka 'blacklisting'). If enough users reveal their usernames and passwords and enough spam comes from the University, the major Internet mail systems may decide to blacklist all traffic coming from tamucc.edu. Getting you or the University off of blacklists is a time-consuming process.

Furthermore, if your mailbox contains confidential information such as grades or social security numbers, then the University must assume that the phisher might have accessed that information. This is called an unauthorized disclosure of confidential information and it often has serious legal consequences. The University is required to report unauthorized disclosures of confidential information to multiple government agencies. This too is very time-consuming and potentially embarrassing for the University.

The phisher installs malicious software on my workstation. Why is that such a big threat to the University?
Even worse is if the phisher convinces you to install malicious software ('malware') on your workstation, such as a key logger. Your workstation is now owned by the phisher. Now the phisher can use your machine to gain access to other machines and services (e.g., Banner, FAMIS) on the network. Now it’s possible for the phisher to access thousands of confidential records, deface a major website, or take control of other machines so as to gain even more control.
Phishing Email FAQ

Why can't IT just stop these phishing emails from getting into my inbox?
In most cases, IT does just that. The University's mail filters stop thousands of obvious spam and phishing messages every week. The mail filters also mark suspicious emails with "{(Spam?)}" or "{(SPF:Fail)}" in the subject line, and you should be extremely suspicious of these messages. However, phishers are always thinking of new ways to get around the mail filters, and thus some phishing emails will come your way sooner or later. Thus, you need to know how to spot them and delete them.

Ok, how do I spot a phish?
There is no surefire way to tell a phish from a genuine email. Instead, there are a number of tell-tales you can look for in an email. The more tell-tales you find, the more suspicious you should be. The tell-tales, in order of importance:

- The email asks you to reply with your username and password. This is absolutely a phish. University IT will never ever ask you for your username and password over the phone or in email.
- The sender's address is strange. If the email says that it is from someone in the University, then the sender's address should end with "tamucc.edu." If instead the sender's address is not @tamucc.edu (e.g., "dwengub@hitech.sg" or "loverboy@yahoo.com") then the email is almost certainly a phish.
- Sense of urgency/dire consequences. If the email says that you must act immediately or your computer/email account will be irretrievably deleted, then the email is most likely a phish.
- Poor English. If the email has run-on sentences, misspelled words, mis-capitalized words, or just reads funny, then the email is most likely a phish.
- The sender doesn't know your name. Phishes are typically addressed to 'Dear User' or just 'ATTN:' or just 'Dear :'. In contrast, a legitimate password change reminder email will typically include your name in the body of the message.

Also, you should be extremely wary when clicking on any hyperlinks within any email. It is trivially easy to insert into an email a hyperlink that displays "www.tamucc.edu" but when clicked takes you to www.telehack.com or some other website. Prudent users don't click on a hyperlink in an email - they manually type the link into their browser.

What do I do if I have an email that could be a phish, but I'm not sure?
Call the Help Desk at x2692.

What do I do if I'm sure I have a phish?
As soon as possible, forward the suspected phish to ITHelp@tamucc.edu (the IT Help Desk) and then immediately call the Help Desk at x2692. Time is of the essence - if you've received a phish, then it's likely that hundreds of other University users have received the same phish. The sooner IT learns about the phish, the sooner IT can counter-act it for everyone.

What should I do if I accidentally fall for a phish?
Change your password and contact the Help Desk at x2692 immediately. Time is of the essence. The sooner IT learns, the better chance we have of stopping the phisher from actually accessing your account or taking other malicious actions. The longer you wait, the greater the chance that something truly bad will happen. If you used the compromised password in other account (e.g., Hotmail, online

Last Updated 2/27/2017
banking), you should change the password in those other sites immediately.

**What will happen to me if I accidentally fall for a phish?**
If IT learns that an account has been compromised (i.e., someone else has acquired the account username and password), IT will immediately disable the account. If the compromise occurred because the user fell for a phish, then the account will be re-enabled only after the user has met with the Information Security Officer in person. Repeated phishing incidents for students will be reported to Student Affairs. Repeated phishing incidents for faculty and staff will be reported to the user's supervisor and on up the organizational chain.

**Is phishing always done with emails?**
No. It can also be done via text messages and over the phone. In the text message case, you receive a text that tells to call a phone number regarding your bank account. Your call is answered by a phisher masquerading as a customer support rep. The second case is where the phisher calls you directly masquerading as ‘the help desk’ and says there’s a problem with your email account and could you please give him your username and password. The TAMUCC Help Desk will never, ever ask you for your password.

**What if I have further questions?**
You can call:
1) Your local IT person
2) The Help Desk at x2692
3) the Information Security Office at x2124.