# Email Security: Phishing



This guide will explain what a phishing email is, how to recognize it, and what you can do if you receive one.

## WHAT IS PHISHING?

Phishing is a type of email (or other communications) where the sender attempts to trick the recipient into giving out personal information, such as account names and passwords, usually by attempting to impersonate official email. Like its homonym, phishing emails cast out many emails hoping that someone will "bite" and fall for their deception. They often use scare tactics to put the recipient off-guard, threatening such consequences as permanently blocking your account or losing refunds to prompt the recipient into acting quickly (and not carefully).

## WHAT DOES A PHISHING EMAIL LOOK LIKE?

A phishing email will attempt to look like an official email, usually from a well-known company like Facebook. It may even appear to come from an SU address. They may hijack and alter an official email, or they may attempt to be more generic, avoiding mentioning a specific company and instead referring to themselves in more general terms like "administrator". They will usually reference some type of account problem, usually concerning the security of your account, and will threaten dire consequences if you do not act immediately.

Cyber-criminals aren't very well known for their spelling acumen, and as such the email will likely contain many spelling and grammar mistakes. Professional companies care about how their emails and correspondence look and at the very least run a spell-check or grammar check on their emails prior to sending, if they aren't employing professional copy editors. Not every email with spelling errors is nefarious, but it is one thing that should raise suspicion.

While links are a popular way to share information via email (and a preferred message for file sharing) you should be suspicious of emails with links in them, especially within unsolicited emails. Phishing emails may use HTML to disguise their link by making it appear to go somewhere else. For example, the text in this link says "http://www.microsoft.com", but the link actually points to http://www.salisbury.edu/helpdesk/security/. You can check this yourself by hovering over the link. In Outlook, this will show in a yellow box by your cursor; in web browsers this usually shows up in the status bar at the bottom of the window.

Keep in mind that phishing isn't limited to email, though it is the most common method. Phone calls and postal mail are also used, though less commonly.

## WHAT SHOULD YOU DO IF YOU RECEIVE A PHISHING EMAIL?

If you think you have received a phishing email, delete it. Don't click on any sort of link, or respond to it at all. You can simply delete these emails. If you wish to report it, you can forward the email to spam@salisbury.edu

## HOW DO THEY GET MY EMAIL?

In most cases, they haven't actually gotten your email address. Most of these spoof addresses, which means that they're generating random combinations and some of them end up being legitimate. Unfortunately, that means that from time to time you get bounce-backs from these.

In other cases, they harvest them from the web (looking for the @ symbol), buying email lists, or getting them from tricking someone you know or have emailed.

## WHAT DOES SU DO TO HELP PROTECT US FROM PHISHING EMAILS?

SU blocks known fraudulent email from ever reaching the campus at our firewall, based on a number of triggers and blacklists (some of which we cover above). Email that is suspicious, but doesn't reach the blocked threshold will receive the subject prefix [SPAM] when delivered, to indicate that it may be spam. Our firewall also blocks certain known bad attachments.

In addition to our security measures, Outlook has built in measures as well, blocking some attachments and employing its own Junk Mail Filter.

However, because of the ever-changing nature of these cyber-criminals, it's impossible to block every phishing email from reaching your mailbox. In order to block every malicious email, we would also have to block legitimate email as well, as many of the factors which indicate a malicious email may also apply to legitimate email, including word triggers, spelling and grammar mistakes, etc.

As such, we take other security measures. Microsoft System Center Endpoint Protection (MSCEP) anti-virus is installed on all campus computers, and is updated and managed by IT on a regular basis. Outgoing mail is also monitored for suspect activity, and email outside of the system is limited to a maximum number of messages per timeframe to prevent spam. Our password security and expiration policies are also a measure to minimize the impact of these emails, and we have pages such as this one and regular emails and communications to the campus as reminders of campus cybersecurity.


Dear Campus Community:

In an effort to help the campus distinguish legitimate emails from the SU Information Technology department from phishing emails w
banner will accompany all official Information Technology announcements sent from the IT Help Desk email account.

If you receive an email that claims or appears to be from a "help desk", "system administrator", "information technology", "the webr
phishing email and you can delete it. If the email does not have the above banner and claims to be from the Help Desk, do not reply
passwords. This should help faculty and staff recognize and filter legitimate Information Technology correspondence sent from the H

**Please report phishing, spam or suspicious emails by forwarding those emails to spam@salisbury.edu.**

Account information sent from pssecurity@salisbury.edu, such as temporary account usernames and passwords, IT Security Agreem
emails from pssecurity@salisbury.edu do not have the above banner, but are still considered legitimate correspondence.

If you believe that you may have given out your login information or suspect your computer or login information may be compromise
5454.

Thank you,

As a final measure, all SU Information Technology emails from the Help Desk have a set banner and style, shown above. If you receive an email asking you for account information that does not have this banner and style, you can delete it. Note that at this time, there are a few exceptions to this: such as password change reminders and emails from pssecurity@salisbury.edu may not have that banner, but are still official. In some cases, such as yearly survey emails, IT will send a preliminary email alerting the campus that the email they receive won't have the banner but will still be legitimate.

## SHOULD I REPORT IT?

This is up to you. If you do want to report these, there are a few places where you can submit your report.

There are a number of government agencies and non-profit organizations that gather these types of emails for investigation. When sending these emails, be sure to Forward as an Attachment when possible, as that will include email headers that are necessary for these agencies and organizations to track the originator's address.

- The Federal Trade Commission (FTC) has set up an email address spam@uce.gov to receive spam and phishing complaints.
- The Anti-Phishing Working Group accepts reported phishing emails at reportphishing@apwg.org.
- The United States Computer Emergency Readiness Team (US-CERT) accepts phishing reports at phishing-report@us-cert.gov.
- If the email is impersonating a specific company, forwarding the email to that company's help or support team may also be recommended.
- You can also forward the email (as an attachment, preferably, to maintain message headers) spam@salisbury.edu.

## WHAT SHOULD I DO IF I RESPONDED TO ONE OF THESE?

If you think you've responded to one of these emails, or clicked on one of the links, there are several things you should do.

- Contact the Help Desk immediately at 410-677-5454 or by forwarding as an attachment the suspected email to spam@salisbury.edu. Let us know how you have interacted with the email (clicked a link, responded, etc.) within the email.
- Change all of your passwords. Reset your SU password at http://mypassword.salisbury.edu. You should also reset any other passwords you have, change PINs, etc.
- Contact your bank about putting a fraud alert on your credit reports. You can contact the credit agencies directly as well; information can be found at http://www.fightidentitytheft.com/fraud_numbers.html
- Close any accounts that may have been compromised, and monitor your accounts for suspicious charges monthly.
- Double-click on the MSCEP logo in your task bar (  ) and choose Scan Now.

## MORE INFORMATION

For more information about phishing, you can check out these helpful websites (where a lot of this information was gathered from):

- US-CERT: http://www.us-cert.gov
- Fight Identity Theft: http://www.fightidentitytheft.com/
- The Anti-Phishing Working Group: http://www.antiphishing.org/
- NakedSecurity from Sophos: http://nakedsecurity.sophos.com/
- BlogsMSDN: http://blogs.msdn.com/b/securitytipstalk/archive/2010/08/06/how-do-spammers-get-my-email-address.aspx