What is Phishing ?

Phishing email messages, websites, and phone calls are designed to steal money or sensitive information. Cybercriminals can do this by installing malicious software on your computer, tricking you into giving them sensitive information, or outright stealing personal information off of your computer.
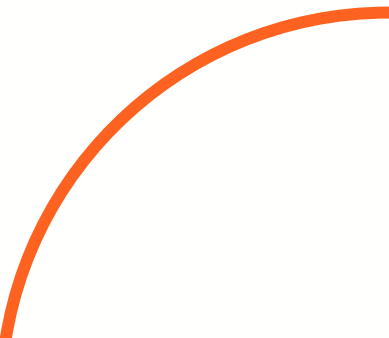
Types of Phishing Attacks

Social Engineering - On your Facebook profile or LinkedIn profile, you can find: Name, Date of Birth, Location, Workplace, Interests, Hobbies, Skills, your Relationship Status, Telephone Number, Email Address and Favorite Food. This is everything a Cybercriminal needs in order to fool you into thinking that the message or email is legitimate.

Link Manipulation - Most methods of phishing use some form of deception designed to make a link in an email appear to belong to the spoofed organization or person. Misspelled URLs or the use of subdomains are common tricks used by phishers. Many email clients or web browsers will show previews of where a link will take the user in the bottom left of the screen or while hovering the mouse cursor over a link.

Spear phishing - Phishing attempts directed at specific individuals or companies have been termed spear phishing. Attackers may gather personal information (social engineering) about their targets to increase their probability of success. This technique is, by far, the most successful on the internet today, accounting for 91% of attacks.

Clone phishing - A type of phishing attack whereby a legitimate, and previously delivered email containing an attachment or link has had its content and recipient address(es) taken and used to create an almost identical or cloned email. The attachment or link within the email is replaced with a malicious version and then sent from an email address spoofed to appear to come from the original sender.
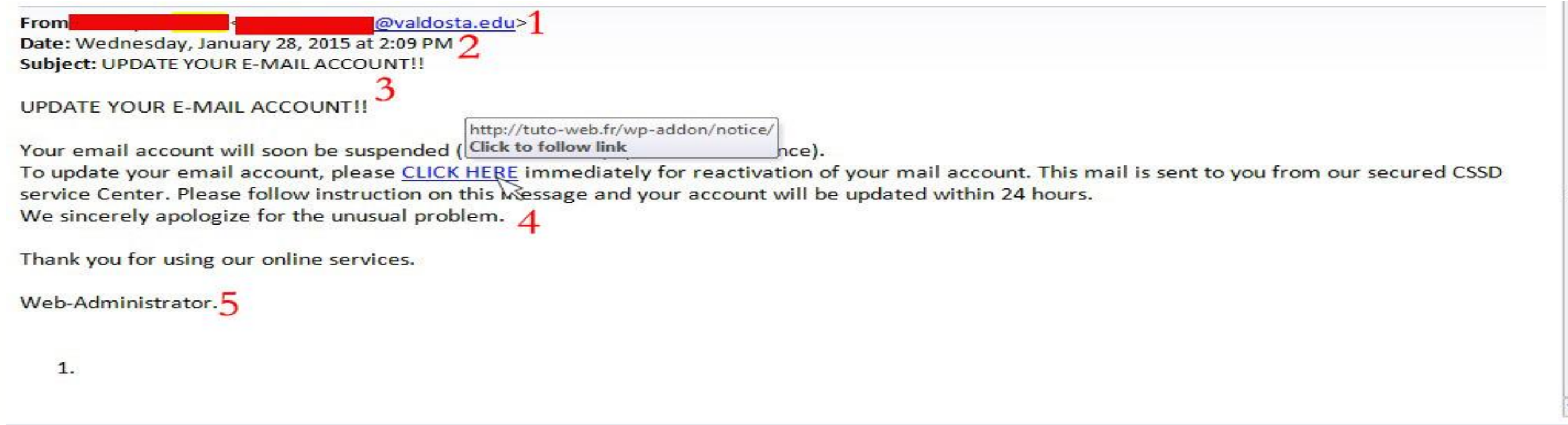
Examples of Phishing Attacks
Spear Phishing

1. The first question you have to ask is, "**Do I know this person**?" or "**Am I expecting an email from the person**?" If you answered no to either question, you must take a harder look at other aspects of the email
2. A large amount of phishing emails will blank out the To: or Cc: fields so that you cannot see that this is a mass email to a large group of people.
3. Phishing emails will often come with subjects that are in all capitals or have multiple exclamation marks in order for you to think that this email is important or that you should take the recommended action within the email.
4. This is a targeted email (Spear Phishing) to VSU, so more than likely, this was sent to everyone at VSU that the sender had in their address book.
5. **Hovering your mouse over the link**, you can see that this is not taking you to a valdosta.edu address, but rather to an external site. This site would either prompt you for a password, then steal that password, or would download a malicious file infecting your computer.
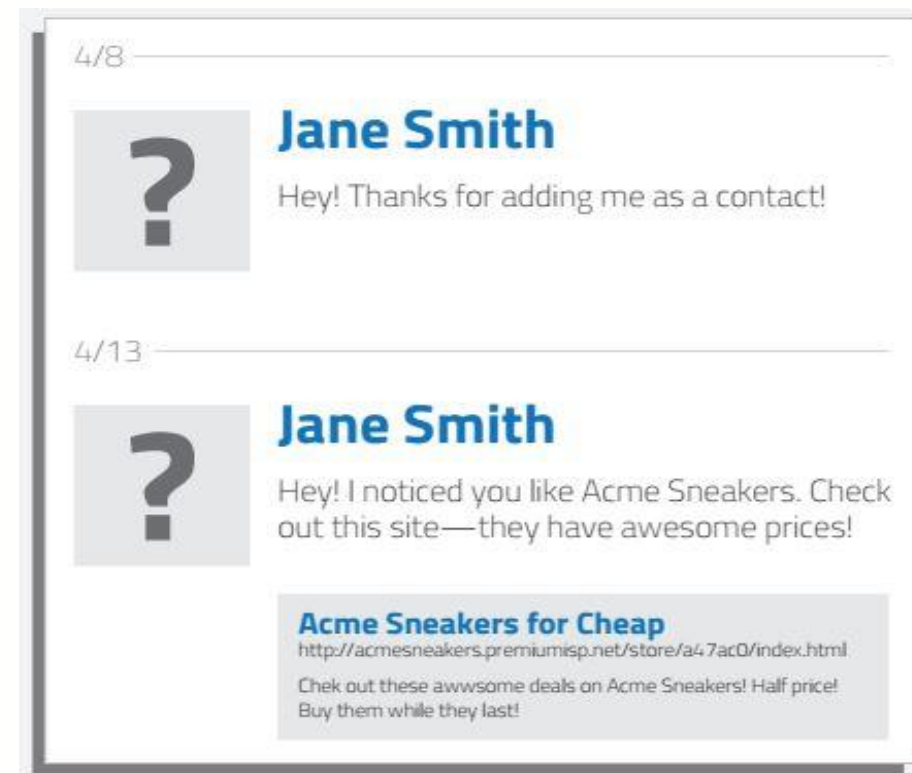
Examples of Phishing Attacks
Link manipulation


```
From                          @valdosta.edu> 1
Date: Wednesday, January 28, 2015 at 2:09 PM 2
Subject: UPDATE YOUR E-MAIL ACCOUNT!!
                                             3
UPDATE YOUR E-MAIL ACCOUNT!!
                                http://tuto-web.fr/wp-addon/notice/
                                Click to follow link
Your email account will soon be suspended (                    nce).
To update your email account, please CLICK HERE immediately for reactivation of your mail account. This mail is sent to you from our secured CSSD
service Center. Please follow instruction on this Message and your account will be updated within 24 hours.
We sincerely apologize for the unusual problem. 4

Thank you for using our online services.

Web-Administrator. 5


    1.
```

1. This is actually from a valdosta.edu address, so first you have to ask whether or not this is from someone you know or someone that would be emailing you about your email account. Remember that **only members of I.T. will email you about your accounts**.
2. One again, cybercriminals will use a subject line trying to get your attention, often using all caps and multiple exclamation marks. **A legitimate email from I.T. will not do this.**
3. The To: and Cc: lines are not shown so that you can't tell this is a mass email targeting multiple individuals.
4. **Hovering your mouse over the link**, you can see that this is not a legitimate valdosta.edu link, but an external one designed to steal your information or install malicious software.
5. The signature often will end in a generic sign off as to not arouse suspicion as to the sender.

Examples of Phishing Attacks
Social Engineering

4/8

Jane Smith
Hey! Thanks for adding me as a contact!

4/13

Jane Smith
Hey! I noticed you like Acme Sneakers. Check out this site—they have awesome prices!

Acme Sneakers for Cheap
http://acmesneakers.premiumisp.net/store/a47ac0/index.html
Chek out these awwsome deals on Acme Sneakers! Half price!
Buy them while they last!

wrote at 12:59pm
Hey check this out!

I just got myself a free $500 gift card to macys

I'm gonna have so much fun!

You all should get one yourself

check out the url below!

http://2url.org/?67562

The example on the left is a targeted social engineering attack. Cybercriminals scan your profile for your likes and then send you a crafted message over social media trying to trick you into clicking the link, which would then steal your social media login and take over your profile sending out more phishing attacks to your friends/contact list.

The one on the right is an example of a mass phishing attack through social media. No doubt many of you have seen these in Facebook, from random people in messages, or from your friends through their timelines. Upon clicking the link, it would prompt you to log in again, but this time to a fake Facebook page, and steal your log in information and take over your profile sending out the same or another mass phishing attack to your friends and contacts.

Can you spot the tell-tale signs of a phishing email?

From: ████████████ @Vanderbilt.Edu>
Sent: Monday, December 8, 2014 6:35 AM
To: ████████
Subject: RE: ITS HELP-DESK

Dear user,

The following evaluations have been assigned to you. Please log in to complete these evaluations.
CLICK HERE TO EVALUATE USING SECURE ENCRYPTION
NOTE: Your log in will time out after 60 minutes. Your responses will be lost if you do not click on the "secure" button before 60 minutes lapses. There is no prompt when your 60 minute session has expired. Please save extensive comments periodically and check your time.

ITS help desk
ADMIN TEAM
©Copyright 2014 Microsoft
All Right Reserved.

Can you spot the tell-tale signs of a phishing email?

1. The email address is not a valid valdosta.edu address, but rather a Vaderbilt.edu address. This is important because **only a valid valdosta.edu address will email you about anything email or help desk related.**
2. The To: and Cc: are missing so that you can tell this is a mass targeted email phishing attack.
3. **Hovering your mouse over the link**, you can see that this is not a valdosta.edu address but rather an external address trying to steal your credentials.
4. The signature is generic as to not alert you to any phishing attempt.

Can you spot the tell-tale signs of a phishing email ?

From: ████████████
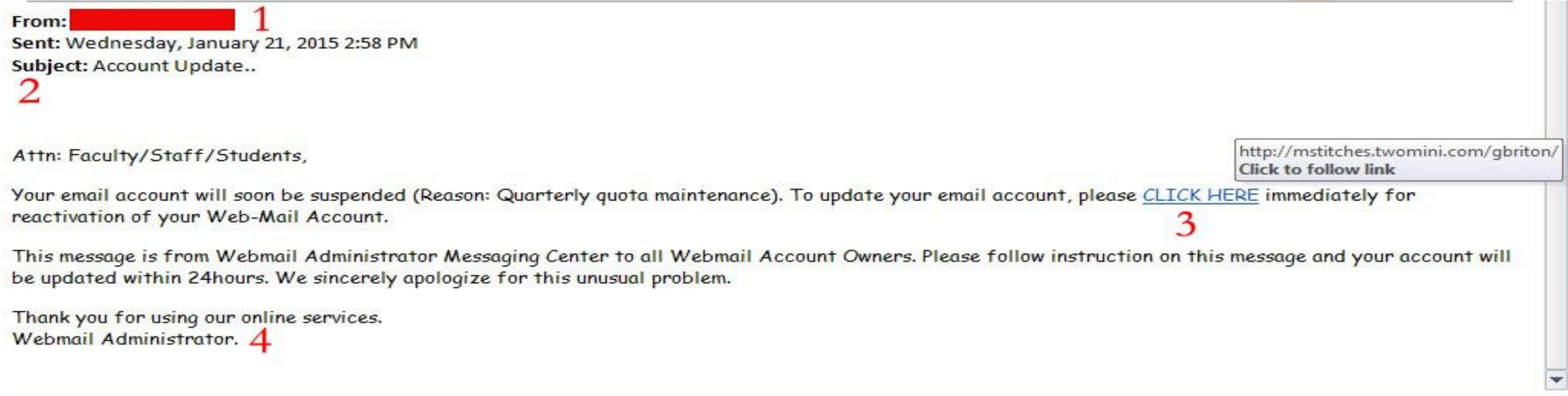Sent: Wednesday, January 21, 2015 2:58 PM
Subject: Account Update..

Attn: Faculty/Staff/Students,

Your email account will soon be suspended (Reason: Quarterly quota maintenance). To update your email account, please CLICK HERE immediately for reactivation of your Web-Mail Account.

This message is from Webmail Administrator Messaging Center to all Webmail Account Owners. Please follow instruction on this message and your account will be updated within 24hours. We sincerely apologize for this unusual problem.

Thank you for using our online services.
Webmail Administrator.

Can you spot the tell-tale signs of a phishing email ?

From: [REDACTED] **1**
Sent: Wednesday, January 21, 2015 2:58 PM
Subject: Account Update..
2

Attn: Faculty/Staff/Students,

Your email account will soon be suspended (Reason: Quarterly quota maintenance). To update your email account, please CLICK HERE immediately for reactivation of your Web-Mail Account.

http://mstitches.twomini.com/gbriton/
Click to follow link
3

This message is from Webmail Administrator Messaging Center to all Webmail Account Owners. Please follow instruction on this message and your account will be updated within 24hours. We sincerely apologize for this unusual problem.

Thank you for using our online services.
Webmail Administrator. **4**

1. The first thing to ask yourself, do I know this person and should they be emailing me about email accounts. If you answered no, then more than likely it is a phishing attempt.
2. The To: and Cc: are not showing so that you wont be able to tell this is a mass email attempting to get as many people as possible.
3. **Hovering your mouse over the link**, you can see that this is not a valid valdosta.edu address, but rather an external address attempting to get your email credentials or install malicious software. This should be your main "Aha" moment to let you know that this is indeed a phishing email.
4. The signature is generic and trying to lull you into a false sense of security by saying this is the "Webmail Administrator"

TIPS TO PROTECT YOURSELF FROM PHISHING

Tips to protect yourself from Phishing emails.

- I.T. will **NEVER** ask for your password over email. Please be wary of any emails asking for passwords. **Never send passwords, bank account numbers, or other private information in an email.**

- Be cautious about opening attachments and downloading files from emails, regardless of who sent them. These files can contain viruses or other malware that can weaken your computer's security. If you are not expecting an email with an attachment from someone, such as a fax or a PDF, please **call** and ask them if they indeed sent the email. If not, let them know they are sending out Phishing emails and need to change their email password immediately.

- **Never** enter private or personal information into a popup window.

- If there is a link in an email, use your mouse to hover over that link to see if it is sending you to where it claims to be, this can thwart many phishing attempts.

- Look for **'https://'** and a **lock icon** in the address bar before entering any private information on a website.

- Look for spelling and bad grammar. Cybercriminals are not known for their grammar and spelling. Professional companies or organizations usually have staff 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.

What to do when you think you received a phishing email ?

- First, **do not** click on any links within the email or download any attachment. Forward the email to abuse@valdosta.edu for Information Security to examine and determine if legitimate.

- If there is an attachment in the email, and you recognize the sender but aren't expecting an attachment from them, please **call** them and ask if it is legitimate.

Signs of a Phishing Phone Call :

- You've been specially selected (for this offer).

- You'll get a free bonus if you buy our product.

- You've won one of five valuable prizes.

- You've won big money in a foreign lottery.

- This investment is low risk and provides a higher return than you can get anywhere else.

- You have to make up your mind right away.

- You trust me, right?

- You don't need to check our company with anyone.

- We'll just put the shipping and handling charges on your credit card.

Tips to protect yourself from Phishing phone calls.

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center, or other watchdog groups.
- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- **Never** send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.

What to do if you think you are receiving a Phishing Call ?

- Always look up the phone number in Google. Often times, others have received these calls before and will log the number and the type of scam to different websites. Some of the websites are 800notes.com, callercenter.com, and callercomplaints.com. Users will let you know whether or not this is a scam, and what the caller will ask for.
- Resist pressure to make a decision immediately.
- **Keep your credit card, checking account, or Social Security numbers to yourself**. Don't tell them to callers you don't know — even if they ask you to "confirm" this information. That's a trick.
- Get all information in writing before you agree to buy.
- Beware of offers to "help" you recover money you have already lost. Callers that say they are law enforcement officers who will help you get your money back "for a fee" are scammers.
- Report any caller who is rude or abusive, even if you already sent them money. They'll want more.

Additional Resources.

http://www.antiphishing.org/

http://www.fraudwatchinternational.com/phishing-alerts

http://phishme.com/

http://www.onguardonline.gov/phishing

http://www.consumer.ftc.gov/articles/0076-phone-scams

http://www.fbi.gov/scams-safety/fraud

Sources

http://phishme.com/phishing-social-media-infographic/

http://en.wikipedia.org/wiki/Phishing

http://www.onguardonline.gov/phishing

Thank you.