

Phishing and Viruses

Essential Understanding:

Knowing how to navigate the web safely gives us the tools to prevent disruptions and security risks when we are online.

Learning Outcome(s):

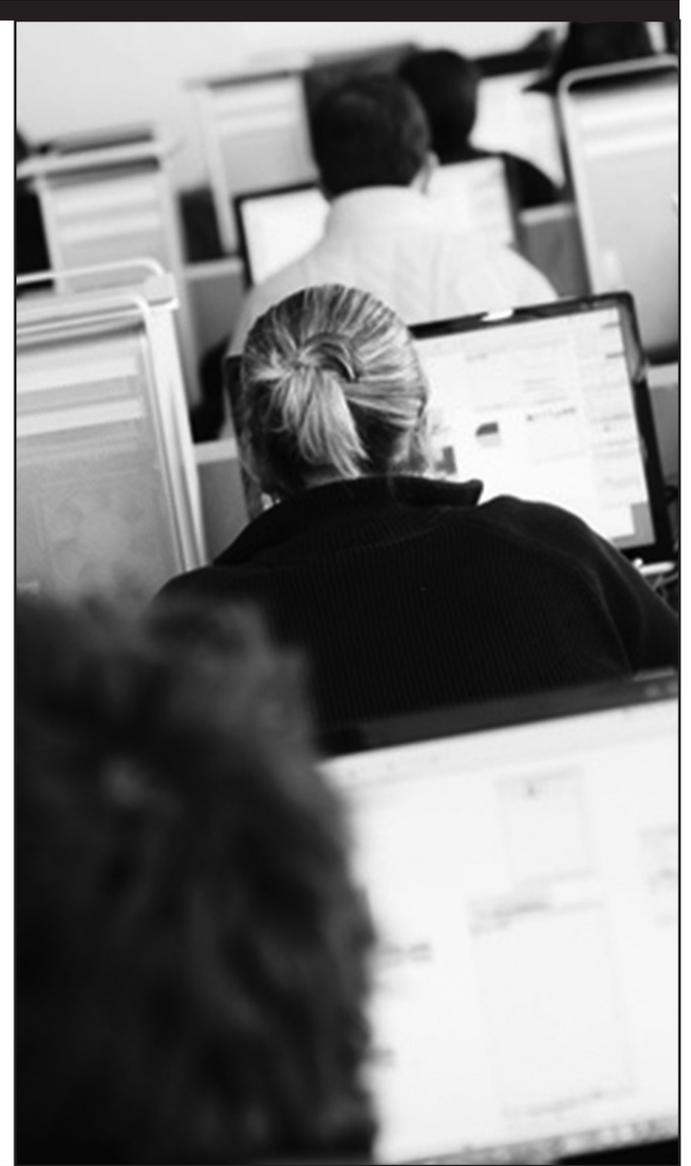
- Students will know and be able to understand the meaning of, ways to identify, and strategies for avoiding instances of phishing and types of e-mail/internet viruses.

Common Core Standard(s):

- SL.9.1.c. Propel conversations by posing and responding to questions that relate the current discussion to broader themes or larger ideas; actively incorporate others into the discussion; and clarify, verify, or challenge ideas and conclusions.

IFC Standard(s):

- Understands and builds on the ideas of others.



GRADE 9

Digital Citizenship Strand: **Safety**

LEARNING/TEACHING ACTIVITIES		RESOURCES
Mini Lesson	Librarian presents power point about phishing and viruses to initiate class discussion of the topic.	PowerPoint Presentation—Phishing Viruses
Guided Practice	Librarian presents examples of phishing, viruses, and other scams: e-mail detailing problem with bank account, etc. Compare and contrast which examples are legitimate and why. Elicit the type of information phishing scams and accidental viruses hope to collect and possible consequences, what signs to look out for in e-mails, “friend requests”, etc.	http://computer.howstuffworks.com/phishing1.htm Phishing and Virus Examples PowerPoint
Independent Practice/Check for Student Understanding	Students work in pairs and look at/read different examples of phishing and viruses to compare and contrast which examples are legitimate and which are not and why.	Handout with Examples
Sharing/Reflection	Pairs share out results and discuss.	
Assessment	Phishing Sheet Students fill out sheet detailing how they will alter their online behavior to avoid phishing and virus scams in the future.	

Follow up/Extensions:

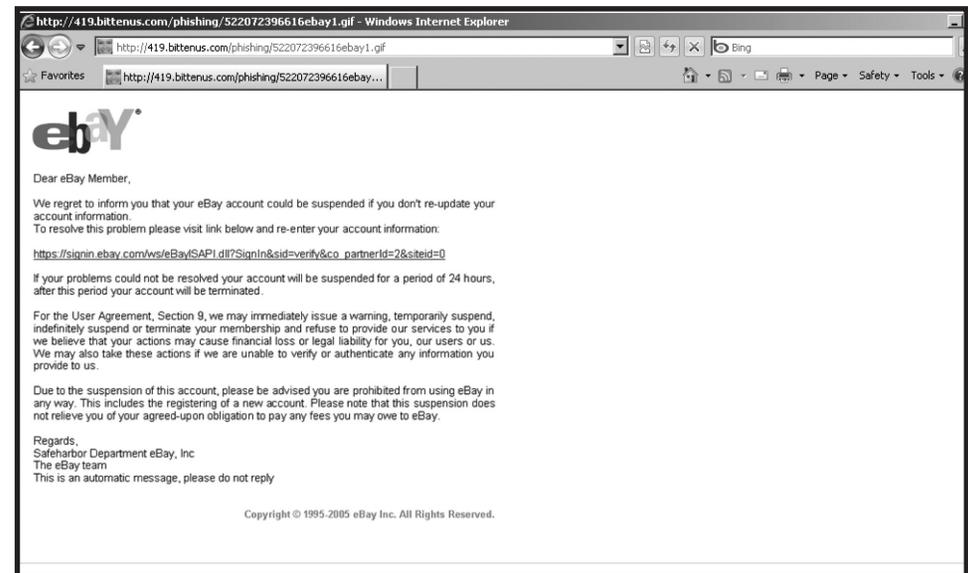
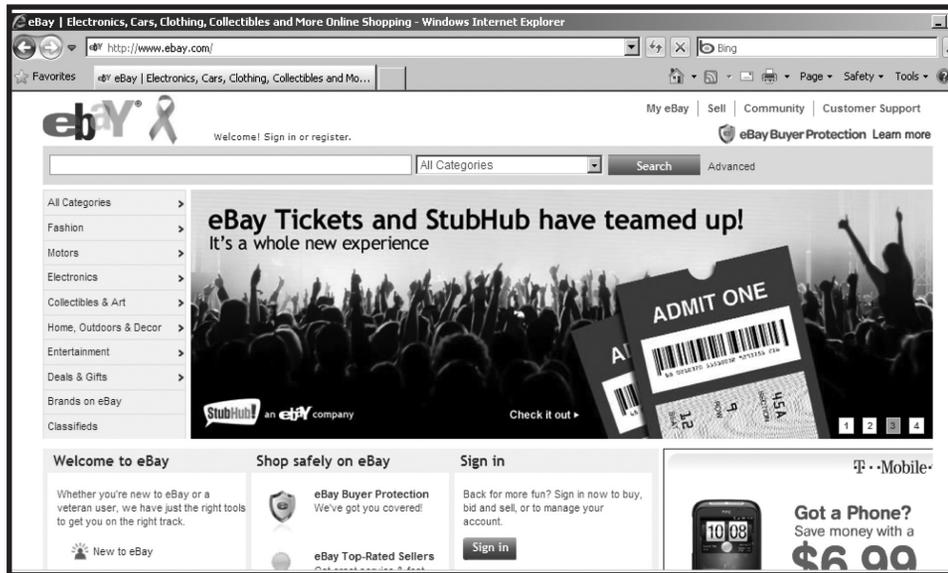
Common Sense Media:

<http://www.common sense media.org/educators/lesson/scams-and-schemes-9-12>

<http://www.common sense media.org/educators/lesson/does-it-matter-who-has-your-data-9-12>

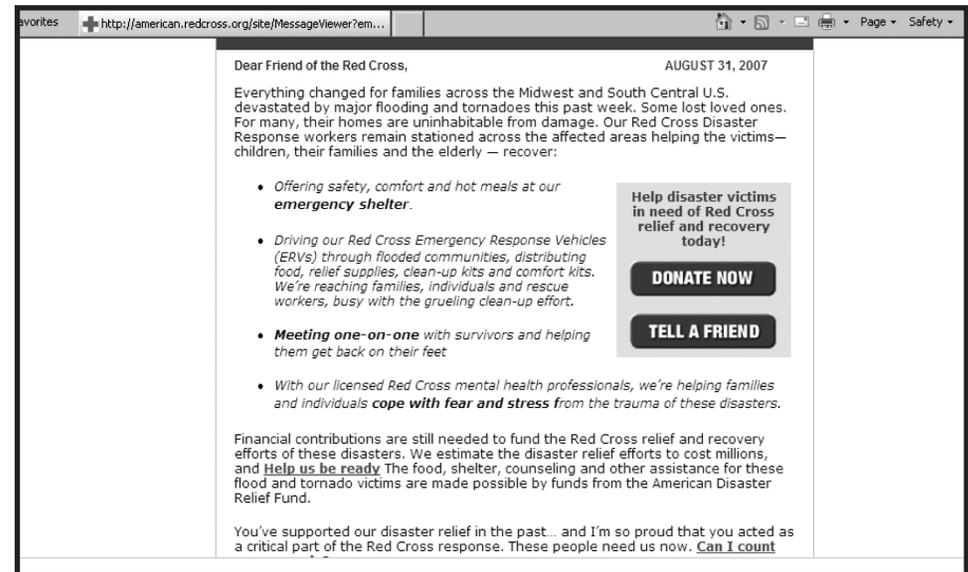
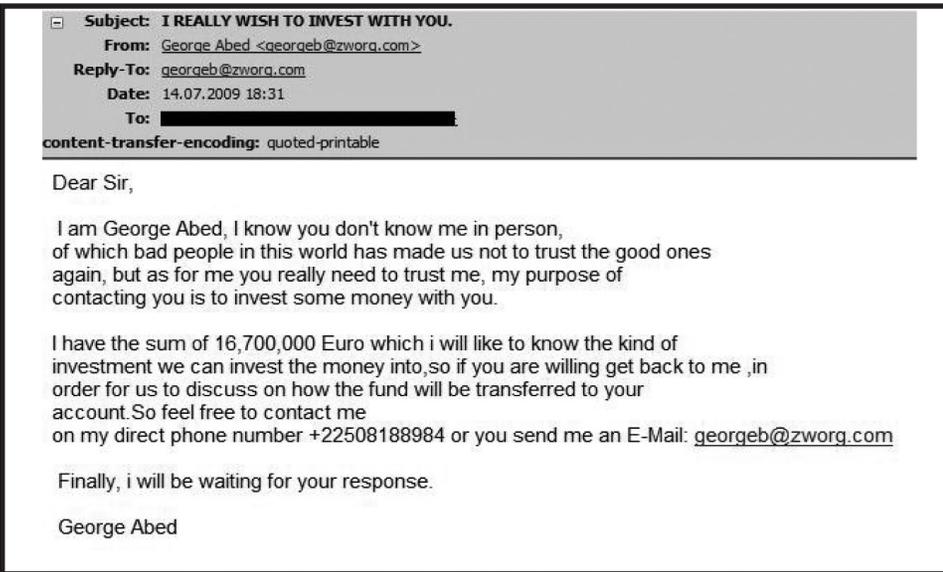
<http://www.ftc.gov/bcp/edu/microsites/onguard/>

Phishing and Viruses Sheet



1. Look at the two examples above. Which one is a phishing example? _____
2. How do you know? _____
3. What is the purpose of the information in the phishing example? *To inform? Persuade? Elicit? Alarm?* _____
4. What are the consequences if a person gives the phishing example the information they are seeking? _____

Phishing and Viruses Sheet



1. Look at the two examples above. Which one is a phishing sample? _____
 2. How do you know? _____
 3. What steps will you take to make certain you will never be a victim of a phishing scam or a virus? _____
- _____
- _____
- _____

Phishing & Viruses



Phishing

Phishing is a way of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.



First recorded use of the term phishing was made in 1996. The term is a variant of *fishing*, and alludes to baits used to catch financial information and passwords.

Communications Purporting to be from

- Popular social web sites
- Auction sites
- Online payment processors
- IT administrators

- Phishing is typically carried out by email or IM
- Usually directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one

Virus

When you listen to the news, you hear about many different forms of electronic infection. The most common are

- Virus (Computer Virus)
- Email Virus
- Worm
- Trojan Horse



© Mark Paris. Permission required for use.

Computer Virus

Viruses - A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.



Email Virus

An e-mail virus travels as an attachment to email messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

ALERT

Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software.

Trojan Horse

A Trojan horse is a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk)



Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid a computer of viruses but instead introduces viruses onto the computer.

Trojan horses may allow a hacker remote access to a target computer system. Once a Trojan horse has been installed on a target computer system, a hacker may have access to the computer remotely and perform various operations.

Worm

A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.



Examples

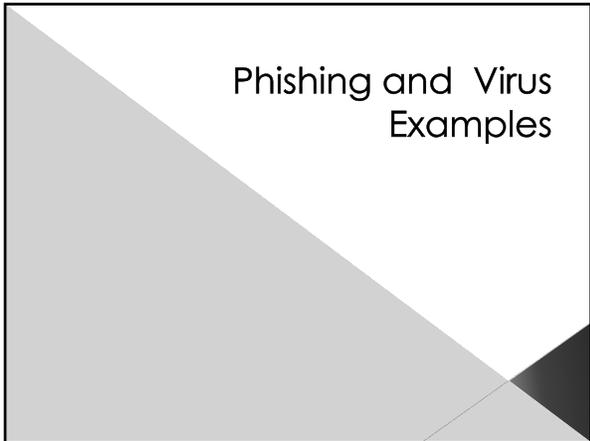
- Mydoom worm infected approximately a quarter-million computers in a single day in January 2004
- Melissa virus in March 1999, was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their email systems until the virus could be contained
- In January 2007, a worm called Storm appeared -- by October, experts believed up to 50 million computers were infected. That's pretty impressive when you consider that many viruses are incredibly simple.

Prevention

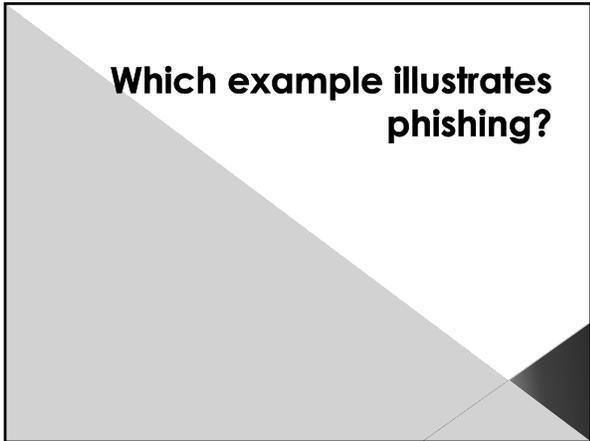
- Software
- Awareness
- Tricks
- Intellect

Common Craft

www.commoncraft.com



Phishing and Virus Examples



Which example illustrates phishing?



Dear eBay Member,

We regret to inform you that your eBay account could be suspended if you don't re-verify your account information.

To resolve this problem please visit the link below and re-enter your account information:

<https://open.ebay.com/verify/545414875/signin&source=partner%26siteid=0>

If your problem could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 5, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Support Department eBay, Inc.
The eBay Team

This is an automatic message, please do not reply.

Copyright © 1995-2005 eBay Inc. All Rights Reserved.



What is the purpose of the information in the phishing example verses the legitimate one?

- Inform?
- Persuade?
- Elicit?
- Alarm?

Phishing Email

Subject: **I REALLY WISH TO INVEST WITH YOU.**
 From: George Abed <georgeab@zworra.com>
 Reply-To: georgeab@zworra.com
 Date: 14-07-2009 18:31
 To: [REDACTED]

content-transfer-encoding: quoted-printable

Dear Sir,

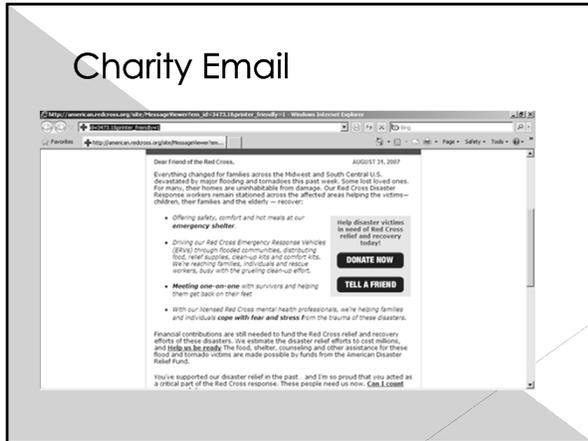
I am George Abed, I know you don't know me in person, of which bad people in this world has made us not to trust the good ones again, but as for me you really need to trust me, my purpose of contacting you is to invest some money with you.

I have the sum of 10,700,000 Euro which i will like to know the kind of investment we can invest the money into,so if you are willing get back to me ,in order for us to discuss on how the fund will be transferred to your account. So feel free to contact me on my direct phone number +22508188984 or you send me an E-Mail: georgeab@zworra.com

Finally, i will be waiting for your response.

George Abed

Charity Email



What information is the phishing email seeking versus the legitimate one?

**Why is the information the phishing email seeks dangerous for the individual?
What could happen?**

