Digital Citizenship Lesson Plan

Avoiding Identity Theft

General Topic (as defined in the Digital Literacy Framework)	**DB8**
Digital Citizenship b) Privacy and Security	
Applicable Grade Range	
6-9	
Outcome(s) to be Addressed	
The student knows strategies for guarding against identity theft and scams that try to access his/her private information online.	
Importance / Significance of Lesson	
Identity theft is a very real threat in today's digital world. Online hackers and thieves are constantly trying to gain access to people's personal information in an effort to manipulate it to their use and gain money and merchandise for free. The effects of identity theft can last years, compromising credit ratings, leading to fraud investigations and causing general frustration in having to prove that you are who you say you are and deal with the hassle of closing and re-establishing accounts with various companies. It is important that students understand the need to protect their information and to be wary of any offers that seem too good to be true.	
Duration	
30 minutes	
Overview	
Students will look at a variety of ways that hackers will try to access their personal information, as well as review news items noting how common hacking attempts are, and then work as a group to develop guidelines to follow in protecting their identity online.	
Required Resources	
Computer hooked up to a projector Class set of laptops/access to the computer lab OR class set of iPads/iPods Copy of the attached resource	

Lesson Plan and Extension Activities

Have students watch (on a computer projected up onto the screen or on their own computers) https://www.youtube.com/watch?v=F7pYHN9iC9I Note that hacking of information is a very real threat in the digital age and it is important that students protect themselves against someone stealing their personal information.

Ask students to identify ways that hackers will attempt to steal their information. Make a list of responses on the board (may include phishing attempts, account confirmation calls or simply hacking into servers that house personal information). Though students can't necessarily protect against their information being stolen from servers, there are things that they can do to protect against their information being stolen in other ways.

Ask students if they have ever heard of 'phishing' and if anyone can explain what it is. Phishing is an email or message sent to someone that typically explains that there is a problem with their account and urging them to login via a link provided in the email to fix their account details. These emails are often from a bank or iTunes or some sort of company that the person does have an account with. The link takes users to a very professional looking website that mimics the official site run by the company, however, when users enter their account information it won't accept the password or somehow creates an error for the user. However, the information that they have entered has already been copied and can then be used against them. A copy of a 'phishing' attempt is attached at the bottom of this lesson plan with identifying information removed. Some glaring concerns come up right away:

1) The price is different in two different places
2) The price of a movie trilogy should never be $199.00
3) The website provides a disclaimer that states 'If this wasn't you, your account has been compromised. Please follow these steps' and then provides a link to the fake website.
4) Though it looks similar to an official iTunes receipt, there are discrepancies.
5) Spelling mistakes are often an indication that something is wrong (poor English skills mean it's likely a fake).

Phishing attempts depend on two things. One, the user's belief that companies would provide this service to protect them, and two, a sense of panic created by seeing that your account has

been closed, charged a large amount of money or compromised. People tend to log in quickly to try to stop further damage, when logging in actually causes the damage.

Ways to avoid falling for a phishing attempt:

1) If you don't have an account with that bank or company, don't worry. It's simply a blanket email sent out to a number of users trying to get you to take the bait.
2) If there seems to be a huge problem – look at it with a critical eye. In the case of the iTunes receipt below, match it up to a real receipt you have received and look for information that is the same or different (hint: they should be exactly the same – except for the price and name of the app or movie ordered – and contain the same account information).
3) Never follow the link in the email. Go to the company's website and log in using your username and password – any suspicious activity will be noted and you can then call customer support yourself. If it is a bank, check for the 'lock' symbol that indicates the site is secure before you enter any information.
4) Track your accounts and usage regularly to catch any purchases or transactions that weren't completed by you.
5) Protect your passwords! Never give out a password over the phone or online unless you made the call yourself or have checked to ensure that the site is legitimate.

Phishing attempts can also be made over the phone by companies who claim to have noted a breach in your account. They will provide some basic information and then ask for an account number or password. These attempts are similar to the above noted email attempts and should be ignored. Tell the representative that you will call the service provider back when you have your information in front of you, look up the company's customer service call center number and have them check your account.

You may also receive emails or phone calls to advise you that you have won something and that you simply need to provide some level of personal information to verify that you are who you say you are. Be very careful providing information – often these are a ruse to get banking information as well. If it looks too good to be true – it probably is!

For further background information, have students look at the news articles listed in the 'Additional Resources' (or look at them as a class). These are just a few examples of hacking attempts that have succeeded on a large scale. Discuss

Have students research ways to protect their identity online and compile a list of tips to follow when using online accounts. Some suggested sites are provided in the 'Additional Resources' section below.

Adaptations

Younger students likely would not have accounts or information that could get hacked and so this lesson might not apply.

Older students would have bank accounts and iTunes accounts that could be compromised. They can do further investigation into news reports of being hacked and provide relevant ideas in how to protect their online identities.

Additional Resources

Tips to protect against identity theft:

http://oag.ca.gov/idtheft/facts/top-ten

http://www.ncpc.org/topics/fraud-and-identity-theft/tips-to-prevent-identity-theft

http://netsecurity.about.com/od/newsandeditorial1/a/aaidenttheft.htm

New reports on identity theft:

http://www.cnn.com/2014/08/06/opinion/rushkoff-russia-hacking/index.html?iref=allsearch Aug 6, 2014

http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html?_r=0 Aug 5, 2014

http://arstechnica.com/security/2014/05/study-97-of-companies-using-network-defenses-get-hacked-anyway/ May 20, 2014

http://money.cnn.com/2013/12/22/news/companies/target-credit-card-hack/ Dec 23, 2013

Cross-curricular Outcomes Also Addressed
Language Arts – read for information, develop guidelines and rules Social Studies – research skills

~developed by Kristin Sward, 2014

iTunes Store <adm@forzan.com.br>

Wed 7/9/2014 7:47 PM

To:

[recipient name];

Billed To:

[recipient email address]

Order ID: 118326068421
Receipt Date: 7/9/2014 4:07:41 PM
Order Total: $199.99
Billed To: [recipient email address]

Item	Artist	Type	Unit Price
Kill Bill Double Feature Report a Problem	Alliance Films	Movie Bundle (HD)	$199.99

Order Total: $19.99

If this was you, then you can safely ignore this email. If this wasn't you, your account has been compromised. Please follow these steps:

Recover Account

You will need to provide your billing information to verify you are the legitimate account holder.

Please retain for your records
Please See Below For Terms And Conditions Pertaining To This Order.

Apple Inc.
You can find the iTunes Store Terms of Sale and Sales Policies by launching your iTunes application and clicking on Terms of Sale or Sales Policies

Answers to frequently asked questions regarding the iTunes Storecan be found at http://www.apple.com/ca/support/itunes/

Apple ID Summary • Purchase History

Apple respects your privacy
Information regarding your personal information can be viewed at http://www.apple.com/ca/privacy/