CyberSmart!
21st century skills for education

ONLINE IDENTITY THEFT:
INFORMATION IS POWER

phishing	**pharming**	**credit report**
driver's license	**pre-approved credit card**	**DOB**
privacy policy	**Social Security number**	**password**
text message scam	**P2P file sharing**	**padlock symbol**

CyberSmart! 21st century skills for education

ONLINE IDENTITY THEFT: INFORMATION IS POWER

GET THE FACTS

What is identity theft?

Identity theft happens when someone uses your private identity information and pretends they are you in order to get money or buy things or services for themselves. Identity thieves steal money out of bank accounts, purchase goods on credit cards, and may even borrow money from a bank by pretending to be you.

Why should I care when I have nothing worth stealing?

Teens and young children are targets for identity theft because they have no credit history. Once the thief uses your name to take out credit cards and bank loans, a history is begun. It's not only the thief's history, it's yours.

How do I know my identity has been stolen?

Not being able to get a driver's license is a clear signal. So is getting *pre-approved credit cards* in the mail when you don't have a bank account or your first credit card. When identity thieves run up big bills and then don't pay them, the result is a bad credit history, which is something that will hurt you when you try to take out your first credit card or get a college loan. Obtaining and checking a free *credit report* once a year is a good way to detect identity theft.

Be CyberSmart!

Your Social Security number (SSN) may be your most precious piece of identity information.

- Don't ever give out your SSN—online or in person.
- Keep your SSN in a safe place. Never carry it with you or put the number in your cell phone or computer.

What information do identity thieves want?

Your full name, address, date of birth (*DOB*), a *Social Security number*, or a *driver's license*. *Passwords* and credit card numbers are also useful, as are cell phone numbers.

How do online identity thieves get my information?

Identity thieves can find your information offline or online. Offline, they may steal mail to get your bank account number or call on the phone and pretend to be from your bank. Online, they may use *phishing*. This is when you or a family member receives an e-mail that looks exactly like one from your bank or other Web site you do business with. It may say that someone is trying to get access to your account or report that the bank needs information about you. It provides a link to a phony site and asks you to verify your private information. The same kinds of requests are made using *text message scams*.

In another kind of scam called *pharming*, you might accidentally download a bit of malicious code that will direct your browser to phony Web sites. When you use *peer-to-peer* (P2P) *file sharing* software in order to share music or movie files, you may also put private identity information on your computer at risk.

What about online shopping?

Shopping online is convenient and allows you to compare prices. When you are ready to shop, type the address of the store into your browser, rather than following a link from an e-mail or pop-up window. If you find the item you want but have never heard of the seller, look for a phone number and then call to see if they answer the phone like a real business. Next read the store's *privacy policy* to make sure they will handle your information with care. Before submitting your name, address, and debit or credit card number, make sure the page on which you type your information is secure by looking for the locked *padlock symbol* at the bottom and/or top of your browser. You should also be able to read the "https" (the *s* means "secure") in the address bar.