iCount

THE ULTIMATE TEEN DESTINATION FOR ALL THINGS MONEY

TEEN QUARTERLY NEWSLETTER

Be Careful When You Click

Free. We all love that word. And when you're online it might be hard to resist free offers you see pop up. But, as your mom and dad probably have told you, nothing is really free.

Whether it's a free app ad on a smartphone or tablet, or a promise of a free game when you're playing online –just ignore it. Downloading these things could give identity thieves access to you or your parent's personal information which could cost them money. Here are a few things you can do to protect both you and your parents when you're online:

- Never give out your name and address
- Never tell anyone your passwords (apart from your mom and dad!)
- Never click on an email attachment unless you know the sender
- Never download anything without checking with mom or dad first
- Never give out your social security number
- Never use a credit card online without your parents there with you
- Never send a photo of you to someone you don't know

We know that many of these tips seem obvious. But identity thieves are getting more and more creative in how they get this information. So you need to get smarter and smarter to beat them!

To find out more about online safety and how to protect yourself, visit the Federal Trade Commission website at http://www.ftc.gov.

Kinds of Internet Scams

You've probably heard online fraud words like "spoofing" and "phishing" before. But do you know what they mean and what they can do to you?

Phishing

Think of the meaning of the regular word "fishing" and you're halfway there to understanding what "phishing" is. With fishing, you have bait that you put on the hook and wait for a fish to be hungry enough to take a nibble on it. With phishing, scammers imitate real companies to get you to share your passwords or credit card information with them (the bait).

If you don't take the time to verify if the email sender is legit, then you'll soon be on their hook and reeled in. Phishers send out millions of emails asking people to verify account numbers or claiming that your online account has been hacked hoping to dupe you into emailing them back with the information they're phishing for. Before you know it, your online accounts have been hacked and your identity stolen.

Spoofing

Spoofing is like phishing, but the sender isn't always out to get you to send them your account information or password - at least not directly.

Spoofing scammers will also email you pretending to be someone else – usually a company that you've had contact with already. (All the better to fool you with!) But instead of asking you to share private information, it will ask you to click on a link. Once you click, you'll be sent to a site that includes innocent looking links that will get you to unknowingly download malware, spyware or other kinds of viruses. Sometimes all these viruses will do is clog up your computer. Other times viruses using spyware will live in your computer and soon find out your passwords and account numbers.

Either scam can have horrible consequences, so please just be careful when you click!