# Hacked Facebook

The Facebook automatic log-ins, most of us use, will allow hackers access to many different site accounts once they have taken over your Facebook. Spammers will also hack Facebook accounts to gain access to your friend following and they can gather a lot of personal information that can be used to steal your identity.

Some signs that you may have been hacked:

- Your name, birthday, email or password has been changed.
- Someone sent out friend requests to people you don't know.
- Messages have been sent from your account, but you didn't write them;
- Posts are appearing on your timeline that you didn't post.

Some steps to take to keep your Facebook account safe:

- Turn on login alerts so that you receive notifications when your account is logged into.
- Enable two-factor authentication, then choose an extra layer of security from the list.
- Choose trusted contacts and add a few close friends or family members that can help you unlock your account if it ever becomes hacked.

With these basic steps, your account is much more difficult for a hacker to get into and much easier to recover if it is ever compromised.

If you feel that your account has been hacked, you can check! On your Facebook page, go to the arrow in the upper right-hand corner of the page and click on it. In the menu, select Setting and a new menu will pop up. In this menu choose Security and Login and then Where You're Logged In.

This will give you a list of devices that you have logged into and their locations will pop up. If there is a login that you do not recognize, chances are, you may have been hacked. If you see anything that is no you, click on the Not You? (right side of the log). Then click on Secure Account. Facebook will then walk you through the steps to secure your account. Click Get Started.

As always, if you have any questions, concerns or comments please do not hesitate to call me at 413-628-4441 extension 1 or stop in at the Department, my door is always open.

Chief Beth Bezio