

Reducing Risks of Cyber Crime

West Noble School Corporation

December 2014

The fury of holiday commercialism erupted last week. First came Black Friday, followed by Small Business Saturday. Then a new week started with Cyber Monday.

There are seemingly endless ways to spend money. This time of year exploits them all.

For those who, for whatever reason, choose not to brave the crowds of the bricks-and-mortar retail marketplace, online shopping has been a godsend. What it lacks in hands-on experience it more than makes up for in convenience. And its popularity continues to grow.

But Internet shopping has its own particular pitfalls, and that's why folks at the Indiana Department of Homeland Security are encouraging people to take extra steps to protect their money - and their identity - when making online purchases.

As headlines over the past year have demonstrated, thieves are becoming adept at hacking into banks and giant retailers and, ultimately, accessing the online accounts of those who've made themselves vulnerable. It's an international problem of growing proportions.

While big-picture solutions will be up to banks and retailers themselves, individuals can play a role by taking action to help protect their own information online. Here, courtesy of state officials, are a few examples:

- Set strong passwords using a combination of uppercase and lowercase letters, numbers and punctuation.
- Change passwords regularly. Set a reminder to change every 30, 60 or 90 days.
- Don't use the same password for multiple accounts.
- Keep operating systems, browser and anti-virus software updated. Patches and updates for software are released when vulnerabilities have been discovered.
- Be cautious of offers online. If it sounds too good to be true, it probably is.

Citizens who believe they are a victim of a cybercrime can take a few steps to respond and recover:

- If there's a problem, disconnect the device from the Internet to prevent an attacker or virus from gaining access to the system.
- If anti-virus software is installed, update the virus definitions and perform a manual scan of the entire system.
- Install appropriate patches to fix vulnerabilities.
- File a complaint with the FBI's Internet Crime Complaint Center at www.IC3.gov.

For more information on cyber security, visit GetPrepared.IN.gov.

While cyber theft is a serious issue, there is no need to shut down your online shopping activity altogether. Taking the actions detailed above will reduce your risk.

Tribune Star. "Reducing risks of cyber crime." *The News Sun* 3 Dec. 2014: 1. Print.