WFG National Title

We Obsess About Cyber Security

Here are ten basic tips that you can use to prevent cybercrime:

1. **Keep computer systems up to date**
   Cyber criminals will use software flaws to attack computer systems frequently and anonymously. Most Windows- based systems can be configured to download software patches and updates automatically.

2. **Protect your computer**
   Be cautious about opening attachments or clicking on links in emails and remember that free apps (games, ringtones, screen savers) can hide viruses or spam.

3. **Keep your firewall turned on**
   A firewall helps to protect your computer from hackers who might try to gain access to crash it, delete information, or steal passwords and other sensitive information.

4. **Protect your personal Information**
   Keep social security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name and date of birth.

5. **Install and update antivirus software**
   Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without the users' knowledge. Most types of antivirus software can be set up to update automatically.

6. **Choose a strong password and protect it**
   Create passwords with eight characters or more and that use a combination of letters, numbers, and symbols. Change your passwords regularly, and don't use the same password for everything. Use second factor authentication if it is available.

7. **Secure your wireless network**
   Wi-Fi (wireless) networks at home are vulnerable to intrusion if they are not properly secured. Review and modify default settings. Public Wi-Fi, a.k.a. "Hot Spots", are also vulnerable. Avoid conducting financial or corporate transactions on these networks.

8. **Review financial statements regularly**
   Reviewing credit card and bank statements regularly will often reduce the impact of identity theft and credit fraud by discovering the problem shortly after the data has been stolen or when the first use of the information is attempted.

9. **Never trust an email, especially with your money**
   If a stranger came up to you on the street and said, "instead of putting that money in your bank, why don't you give it to me and I'll take care of it for you." Would you believe that person? Of course not; that is precisely the same thing as getting an email telling you to send your money to a particular bank, especially if it's a change from instructions you've already received. Email is not secure; it is virtually impossible to tell who an email actually came from. Whenever money is involved, always call to confirm the instructions are correct before you send the money.

10. **Turn off your computer when not in use**
    With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible to attack by cyber criminals.