

Monthly Columns

by Attorney General Jack Conway



January 2011

Online criminals work day and night to steal identities, personal financial data and any other information they can profit from. Each year, as many as 10 million Americans fall victim to identity theft. It is the fastest growing crime in America, costing businesses and consumers more than \$55 million in fraudulent charges annually.

In today's technology-driven world, it is more important than ever to protect your personal data by checking privacy settings on social websites and using secure networks.

According to a recent industry study, 21 percent of adult social network users leave their profiles open for anyone to see—that's more than 24 million Americans who are putting their financial security and their safety in jeopardy. The same study found that 70 million people have shared their birthplace and birthdates on social websites, while 20 million have shared their pet's name. This is the very information many people are asked to provide when setting up bank accounts.

Social network websites, such as Facebook, allow users to limit who can view the personal information in their profiles. Please make sure to check your privacy settings and always think before you post. Comments you make online can affect your employment, admission to college, your friendships and even your safety. A 2009 study found that 70 percent of human resources professionals have rejected a candidate based on what they found out about a person following an online search.

Also, think twice before you post information about your vacation plans. Posting vacation updates on an open website tells the world, and possibly a burglar, that your home is vacant.

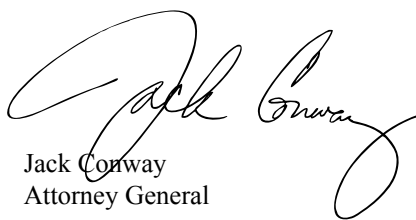
Configuring your wireless router to encrypt data is another important step in protecting your personal data on the Internet. Manufacturers often deliver wireless routers with the encryption feature turned off. Always activate your router's encryption feature. This helps ensure that information you transmit over the web, such as account logins, passwords and

credit card numbers, is scrambled.

Make sure to read the instructions that come with your wireless router to determine how to turn on the encryption feature. Two main types of encryption are available; WiFi Protected Access (WPA) and Wired Equivalent Privacy (WEP). It is also important to use anti-virus and anti-spyware software and a firewall. For help configuring your router, visit www.onguardonline.gov/topics/wireless-security.aspx.

Although café, hotel and airport "hot spots" are convenient, they are not necessarily secure. You should assume that other people can see anything you see or send over a public wireless network. For additional information on how to protect your safety online or the safety of a teen or senior citizen, please visit my Cybersafety in Kentucky page at <http://ag.ky.gov/cybersafety>.

By following these simple steps, you can better protect yourself against online fraud and identity theft and help me make the Internet a safer place for all Kentuckians.



Jack Conway
Attorney General