



Work-at-home schemes attract otherwise innocent individuals, causing them to become part of criminal schemes without realizing they are engaging in illegal behavior.

### **Protection against malicious acts:**

- Consumers always need to be alert to unsolicited e-mails. Do not open unsolicited e-mails or click on any embedded links, as they may contain viruses or malware.
- Consumers are advised to do as much due diligence as possible before engaging in transactions to purchase vehicles advertised online. Consumers are also cautioned to be aware of the rules or warnings posted by the Internet sites they visit. If someone is asking you as a consumer to break or avoid the rules of the website, it is possible that person is trying to scam you.
- Job scams often provide criminals the opportunity to commit identity theft when victims provide their personal information, sometimes even bank account information, to their potential "employer." The criminal/employer can then use the victim's information to open credit cards, post on-line auctions, register websites, etc., in the victim's name to commit additional crimes.

If you have been a victim of Internet crime, please file a complaint at [www.ic3.gov](http://www.ic3.gov).

Other scams and computer crimes that consumers should understand and should be made aware of:

### **■ Data Manipulation**

Changing data during or after input into a computer system is the simplest, safest, and most common method of committing computer crime. This process can be performed by anyone who has access to the process. This includes creating, reordering, transporting, encoding, examining, checking, converting, or transforming the data that was originally entered.

### **■ Salami Technique**

Employees engaging in white-collared crimes who work for financial institutions usually use this particular term. This technique is trimming off small amounts of money from many sources and diverting these slices into one's own or an accomplices' account. With this type of Internet crime, an individual can skim off of many accounts daily for 1 year.

### **■ Trojan Horse, Viruses, and Worms**

All of these methods are extremely common. The Trojan horse is slick and sly. At first the Trojan appear to behave and act as if it is doing what the computer operator expects, but it contains a code that allows and invites other viruses onto the computer. The virus infects programs, while the worm just takes over computer memory and denies its use to legitimate programs.

### **■ Electronic Eavesdropping**

Tapping, without authorization, into communication lines over which digitized computer data and messages are being sent.

### **■ War Driving**

This term refers to hackers driving around searching for wireless networks.

### **■ Identity Theft**

Identity theft could be defined as using information stolen from computer databases, and criminals utilizing the information stolen as if it's there information.

### **References**

- Bartol, C. R. & Bartol, A. M. (2005). *Criminal Behavior* (7th edition). New Jersey: Prentice Hall
- Dalton, D.R. (2003). *Rethinking Corporate Security in the Post 9/11 Era*. Boston: Butterworth Heinemann
- Green, G. & Fischer, R.J. (2004). *Introduction to Security*. Boston: Butterworth Heinemann
- Panko, R.R. (2004). *Corporate Computer and Network Security*. New Jersey: Prentice Hall