Cybercrimes

Read the fine print on website privacy policies—On many social networking and photo-sharing sites, there is wording on the privacy policies that allows the website to keep information and photos posted to the site, sometimes indefinitely, even after the original has been deleted by the user. While this may not discourage one from posting images or messages, awareness that this can be later retrieved and disseminated may be a consideration as to what information or photos are posted. What today may seem to be a harmless prank can have a devastating effect on one’s reputation several years later when applying for a job or other opportunity.

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. Credit card protection services can often alert a person when there is unusual activity occurring on his or her account, for example, purchase in a geographically distant location or a high volume of purchases. These alerts should not be taken lightly and could be the first indicator that a victim receives that something is wrong.

If it seems too good to be true, it is—No one is going to receive a large sum of money from a dead Nigerian politician, win a huge lottery from being “randomly selected from a database of email addresses,” or make big money from “passive residual income a few hours each day working out of your home.” Many of these crimes go unreported because the victim is too embarrassed to admit to law enforcement that they were duped.

Turn off your computer—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. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker’s connection—be it spyware or a botnet that employs your computer’s resources to reach out to other unwitting users. (FBI Website - Scams and Safety, How to Protect Your Computer: www.fbi.gov/scams-safety/computer_protect)

The bottom line is for every preventative measure that you take, you limit your chances for becoming a victim of cybercrime.

Resources

Federal Bureau of Investigation (FBI) for cybercrime information

www.fbi.gov/about-us/investigate/cyber
Federal Bureau of Investigation (FBI) for tips to avoid Internet fraud www.fbi.gov/computer-crimes-fraud
Internet Crime Complaint Center www.ic3.gov
Department of Justice - Computer Crime and Intellectual Property Section www.cybersite.gov
Federal Trade Commission Consumer Information www.ftc.gov/bcp
National Crime Prevention Council www.ncpc.org

Also, contact your local police department for information on local cybersecurity issues and prevention suggestions.

BIBLIOGRAPHY


This project was supported by Grant No. 2009-GP-BX-K052 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Community Oriented Policing Services. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice.

Copyright © 2012 All rights reserved. Printed in the United States of America September 2012
Knowing the facts, trends, and cybercrime trends and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.

In 2011, the annual cost of identity theft was $37 billion dollars—Identity Theft and Fraud and release annual reports on the statistics and cybersecurity facts in its RealID and facts and figures report prepared on cybersecurity trends and growth. Knowing the facts, trends, and growth is critical to crime prevention efforts on protecting personal data as well as public sectors. This also helps in the creation of tools and strategies to combat cyber criminals.

Internet connected activities are as vulnerable to crime as they can lead to victimization as effectively as common physical crimes. The types of crime that are currently occurring have existed long before the Internet was around. By virtue of the tools being used today to connect criminals, criminals are now anonymous and prevented from using a virtual mask or avoiding victimization. The responsibility falls on individuals to protect themselves and their families through safe online practices.