
CYBER
CRIME
EXPOSED

CYBERCRIME
EXPOSED

Written by **Marian Merritt**,
Symantec's Internet Safety Advocate

Contents

The Cybercrime Threat

Your safety is in your hands **1**
The impact of cybercrime **2**
Symantec's Internet Security Threat Report. **2**
Cybercrime, from chaos to commerce. **4**
The hacker generation. **4**
The criminal generation. **6**

The Cybercrime Risk to You

Your information is at risk. **7**
Spam is on the increase. **8**
Phishing for dollars—your dollars. **8**
The drive-by download. **9**
Utilizing weaknesses in your software. **10**
Beware of Trojan attacks and online auction scams. **10**
A different kind of cybercriminal. **11**

Protecting Yourself Against Cybercrime

Develop a comprehensive defensive strategy. **13**
Norton from Symantec, detecting and protecting against cybercrime. **13**
Norton 2010, defending your digital rights. **13**

Glossary. **15**
Resources for victims of cybercrime. **17**

For more information about Cybercrime and Norton 2010 products, please visit **www.everyclickmatters.com**

The Cybercrime Threat

Your safety is in your hands

It's dark, in the hours before dawn. You are alone in your car, speeding down a highway. Headlights appear in the distance. With a sudden jolt of adrenaline, you realize the lights belong to a car in your lane. A car is driving the wrong way. You are headed for a certain head-on collision unless you take quick and decisive action. Quick, you have seconds to react; will you swerve left or right? Will you crash or not?

Every click matters

The online world of cybercrime presents equally critical decisions for you to make, but there are no obvious signs like oncoming headlights. Instead, you get a silent "security warning," a link with a tempting offer, or a text message from a known sender. Will you choose the right option or will you be attacked? Will you "Allow" or "Deny" the cybercriminal to have their way with you? In today's online world, every click matters.

Everyone who goes online is vulnerable. The bad guys are out there. They're organized, sophisticated. And the impact of their actions is broad and devastating. In fact, cybercrime is so pervasive, it's estimated to exceed the revenues of international drug trafficking.[1]

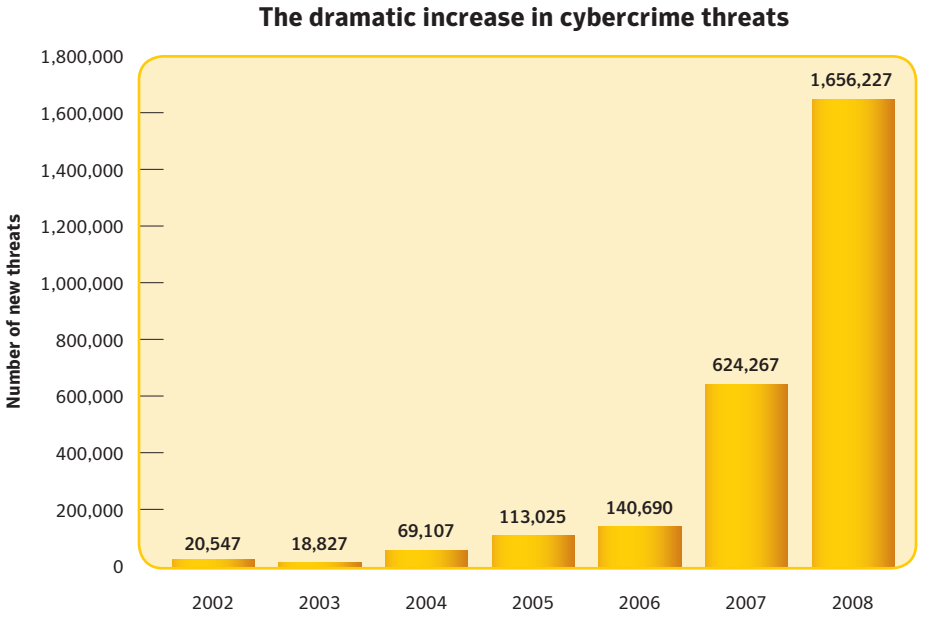
1. http://www.securitywatch.co.uk/2009/03/26/cybercrime-revenues-exceed-drug-trafficking/

The impact of cybercrime

- Conficker/Downadup worm infects 50,000 computers each day.[2]
- Roughly half of online adults have either lost irreplaceable data from a hard drive crash or had someone break into their computer.[3]
- Fake emails will cost consumers like you more than $140 billion in 2009.[4]

Symantec's Internet Security Threat Report

At Symantec, our researchers cover the globe to detect, measure and develop defenses against all forms of cybercrime. Symantec's Internet Security Threat Report covers Internet threat activities, vulnerabilities, malicious code, phishing, spam and security risks as well as future trends. And it provides a disturbing window into the impact of the underground criminal economy on consumers and industry.



2. http://www.computerworld.com/s/article/9133363/Conficker_still_infecting_50_000_PCs_per_day
3. http://www.nortononlineliving.com/
4. http://www.ferris.com/?p=322011

Symantec has established some of the most comprehensive sources of Internet threat data in the world through the Symantec™ Global Intelligence Network. This network captures worldwide security intelligence data that gives Symantec analysts unparalleled sources of data to identify and analyze, to deliver protection and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam.

More than 240,000 sensors in 200+ countries monitor attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services and Norton™ consumer products, as well as additional third-party data sources.

Symantec gathers malicious code intelligence from more than 130 million client, server, and gateway systems that have deployed its antivirus products. Additionally, Symantec's distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attacker methods.

The cybercrime black market

- There is now an underground cybercrime economy, an Internet black market where today's cybercriminal can buy, sell, barter and trade criminal skills, tools, and your private information.
- Cybercriminals now are less like hackers and more like offline crime syndicates, such as the Mafia or urban gangs.

On sale today: your ID and the tools to steal it

- On the Internet black market one can buy everything from IDs and credit cards to botnet kits, RFI scanners, autorooters, shopadmin exploiters, and more.
- These kits enable even rookie criminals with limited resources to buy malicious code and as many as 100,000 IM addresses.
- Here are a few examples—one can buy a keystroke logger for about $23 or pay $10 to have someone host a phishing scam. Pick up a botnet for just $225. Or get a tool that exploits a vulnerability on a banking site for $740 to $3,000. Even if a virus is only picked up by 1% of the people it is sent to, that is still a good return on investment.

Your personal information is under attack

- Malicious code that can export your personal data accounted for 78% of threats to confidential information in 2008, up from 74% in 2007.
- Confidential information threats with a keystroke-logging capability made up 76% of threats to confidential information, up from 72% in 2007.

Credit cards are the primary target

- In 2008, credit card information accounted for 32% of all goods advertised on the underground economy. This was an increase from 21% in 2007.
- Credit card information advertised on the underground economy consists of credit card numbers and expiration date, and may also include the name on the card, billing address, phone number, CVV2 number, and PIN.
- Credit cards were sold in the underground economy for $0.06 to $30 per card in 2008, depending on the amount of information included with the card, rarity of the card type, and bulk purchase sizes.

Bank accounts are close behind

- Bank account credentials accounted for 19% of all advertised goods in 2008. This was a slight increase from 17% observed in 2007.
- The advertised price for bank account credentials varied, with prices ranging from $10 to $1,000 depending on the amount of funds available, the location of the account, and the type of account.

Cybercrime, from chaos to commerce

If you thought viruses were written by hacker kids in their mother's basements, you're in for quite a shock. Let's review with a recap of some cybercriminal profiles and top types of online crimes.

The hacker generation

In the early days of cybercrime, the criminal's intent was to create chaos and destroy. The first virus writers sought notoriety, not money. In 1999, David L. Smith created the "Melissa" virus which infected computers with an estimated $80 million in damage, but did not drive any criminal revenue for Smith.[5]

Jeffrey Lee Parson created the "SoBig" worm in 2003. He was only 18 years old, yet SoBig was one of the fastest spreading viruses and caused an estimated $50 million in damages in the U.S. alone.

5. http://pressroom.consumerreports.org/pressroom/2009/05/consumer-reports-survey-one-in-five-online-consumers-have-been-victims-of-cybercrime.html

Tips:

- Use a state-of-the-art integrated security software suite, such as **Norton™ Internet Security** or **Norton 360™**. It's not always sufficient to use just an antivirus; you need firewall, identity protection, intrusion prevention, and more.
- Maintain vigilance with your operating system and browser. Make sure you're using the latest version and configure each to automatically update with patches and security fixes.
- Be cyber-street savvy—don't click on links in email, Instant Messaging, social networks, or even text messages on your phone without double checking with the sender.
- Don't fall for the fake "antivirus" security alerts or advertising that continue to propagate online. Often, the "scamware" is worse than any virus, doing nothing to protect you, while at the same time, ripping you off.
- Back up your computer and important data. Prepare today for a crisis tomorrow. **Norton™ Online Backup** is a great and easy way to secure your data online, which also gives you remote access to all of your backed up files through the Web via any computer.

The criminal generation

Today, online threats are very different from those early viral creations. Current cybercriminals simply want to make money. Lots of it. And despite the efforts of law enforcement, they do.

The Gonzalez hack

In 2007, credit card systems of a major U.S. retailer were attacked. A syndicate of hackers breached the credit card systems, stealing the credit card information of approximately 45 million consumers. The private information of 450,000 customers, including Social Security numbers and driver's license numbers, was also accessed by the criminals, apparently due to an insecure wireless network or stolen encryption information. The apparent kingpin of the group, Albert Gonzalez, also known by his hacker name as "CumbaJohny" and "Segvec," was a double-crossing FBI informant who used insider information to help his fellow criminals evade detection. One of the key programmers who wrote the successful code was Stephen Watt. Though the criminal use of the data was only estimated at several millions of dollars, the cost to repair the damage has already reached $130 million.

Trading on your information

Once information is stolen from data breaches like the Gonzalez hack or lesser known breaches from lost or stolen laptops, misplaced data disks or data stolen by employees, that information often gets traded on the underground black market. One such hacker/trader who got caught was Ehud Tenenbaum. He made at least $10 million off of stolen credit card information gained from his hacking efforts. He, like so many others, turned to the underground criminal economy to find those who could "cash" the card, in effect, purchase goods for resale as quickly as possible before the credit holder or the banks became aware of the breach.

The Cybercrime Risk to You

Your information is at risk

Modern cybercrime, as we said earlier, is about money. 78% of online attacks include a financial component and, in fact, 76% of those online attacks include a keystroke logger—a piece of software that silently waits on your computer to record your logins and account credentials and passwords and then ships them off to the crooks, wherever they may be, via the Internet. Next thing you know, your bank account is being emptied and your credit cards are being used fraudulently.

Key facts

- If you are a victim of identity theft, you'll spend an average of 58 hours recovering losses.[6]
- 90% of digital threats are an attempt to steal your private information.[7]
- 1 in 5 online consumers were a victim of cybercrime.[8]
- 7 million people like you were tricked into giving personal information to cybercriminals over the last two years.[9]

Tips:

- Guard private data—be careful who has access to your personal information like Social Security numbers, account data, and passwords.
- Review bank, investment, even online auction payment accounts diligently. Sign up for fraud alerts on your credit cards. Check your statements carefully each month or online.
- Manage your credit report. You can order a free copy from each of the three U.S. credit report agencies per year. Make sure no one is using your hard-earned credit for their personal gain.

6 .http://www.idtheftcenter.org/artman2/publish/m_press/Identity_Theft_The_Aftermath_2008.shtml
7. http://www.symantec.com/about/news/release/article.jsp?prid=20090728_01
8. http://pressroom.consumerreports.org/pressroom/2009/05/consumer-reports-survey-one-in-five-online-consumers-have-been-victims-of-cybercrime.html

Spam is on the increase

More than 9 out of 10 of the world's emails are fraudulent. No doubt, you've noticed the increased amount of spam. The spam keeps coming because it works. People do click on the messages, fill in their account details, order the fake pharmaceuticals and sign up for bogus work-from-home schemes, and lose their personal information. Additionally, the new popularity of botnets (easily found in do-it-yourself kits online) to send spam out from infected computers keeps law enforcement hopping as they try to track down the sources of spam.

From the late 1990's through 2008, so-called "spam king" Sanford Wallace and his partner Walter Rines wreaked phishing and spam havoc on the users of social networking sites. Innocent visitors to fake profiles might expect to have spyware installed on their computers, then were offered to have the criminals remove it for $30. Some of their other malicious efforts promoted porn and gambling sites.

Another spammer, Jeremy Jaynes, was the first to be convicted of felony spamming. At the height of his criminal efforts, he was sending hundreds of thousands of bogus email ads every day from thousands of fake email accounts. It was estimated that he was earning $750,000 per month from his spam ads. In 2003, Congress enacted the CAN-SPAM Act to criminalize unsolicited electronic advertising, but despite this and the efforts of ISPs and consumers, spam only continues to grow as a problem.

Phishing for dollars—your dollars

Phishing attacks, or fake email or other lures that get the consumer to provide confidential data, are rising by as much as 20% a month, according to Symantec's July 2009 State of Phishing report.[10] One creative phishing attack offered Australian tax payers a special printable form to access their refund payments. After the victim entered their sensitive financial information into the form and clicked "Print," their private data was sent to the cybercriminals. Fortunately, the Australian tax authorities discovered the fraud and worked diligently to shut down the servers hosting the attack.

More typical are those forms of online fraud that play upon our interests, emotions, and concerns. Cybercriminals know to use "social engineering" to trick us into lowering our defenses. While we're donating to a charity, our credit card is actually being charged by a criminal account. Or perhaps, while we're looking at porn, a salacious video or photographic content—instead of the juicy details we think we're downloading—we're actually downloading a keystroke logger or bot onto our own computer.

10. http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_07-2009.en-us.pdf

Tips:

- Use spam filtering, offered by your email provider and standalone services. Never click an email offer or reply to the sender, even to register a complaint. Make sure children know to avoid clicking on emailed offers in their email accounts.
- Use strong security software to help you avoid clicking on links that take you to infected and malicious websites. Avoid URLs that have been shortened if you can't preview where it will take you.
- If you need to visit a website to address your account status, type the address in yourself. When prompted for an unexpected download, like a video player, refuse the download and research at the manufacturer's site to see whether your program needs an update.

An increase in Web-based attacks

- Web-based attacks are now the primary mechanism for malicious activity over the Internet.
- Cybercriminals infect legitimate websites with malicious code. They're often able to do this due to a vulnerability on the website's end. All a computer user has to do is visit the website or click on something on the website and they can be infected.

The drive-by download

Cybercriminals get you as you go about your daily routine by infecting legitimate websites that have failed to maintain good security on their site. They will either try to drop infected content onto your computer or will redirect your browser to another site, managed by the criminal. If the insecure application or server is a commonly used one, that single vulnerability can allow crooks to infect thousands of websites and impact millions of users.

We've seen examples of the "drive-by download" on infected sites like the Miami Dolphins' ticketing site[11] and individual pages of social networking sites, such as the page for R&B recording artist Alicia Keys.[12] Users need to be cautious at all times when online about accepting downloads or clicking on security alerts.

11. http://www.networkworld.com/news/2007/020207-dolphins-web-sites-hacked-in.html
12. http://www.theregister.co.uk/2007/11/09/myspace_trojan_hack/

Utilizing weaknesses in trusted software on your computer

"Patch Tuesday" may not appear on your calendar, but it should. It's the day that Microsoft issues important security and other patches for their operating systems. Similar efforts exist from every OS or software vendor and should be an important part of every user's protective effort. Install available patches as soon as you can to be sure your system is protected. Conficker or Downadup infected millions because they hadn't taken that step or couldn't because they were using illegal copies of Microsoft® Windows.®

Tips:

- Use strong security software such as **Norton Internet Security** and website rating systems like **Norton Safe Web**.
- Keep your operating system and browser software in shape by downloading and installing patches and upgrading to the latest, most secure versions.

Beware of Trojan attacks and online auction scams

On a daily basis, we purchase goods and services online. Using an online auction or searching for desired items online shouldn't be a risky activity. But threats such as click fraud Trojans can make shopping dangerous. Each works in a slightly different way. For example, a click fraud Trojan may kick off with a legitimate online ad for a car. When you email the seller, the reply you receive will download a Trojan onto your computer. From then on, any effort to review the online auction or research the seller at the auction site is intercepted by the criminal who is able to steal your financial information while displaying fake Web pages making their seller feedback look great, and showing other bids for the car.[13]

In another version of this scam, the downloaded program intercepts online searches in Google, sending you returned search results that lead to the cybercriminals' sites, though the search results look legitimate.

A low-tech version of these scams includes fraud in online auction and local trading sites where goods are never delivered. Some scammers contact you after you fail to win the desired item in an auction, claiming to have additional copies, but they've actually created a duplicate auction page in order to defraud you. Or the criminal will ask you to use an alternate payment method, which fails to adequately protect you from crime.

13. http://www.symantec.com/connect/blogs/how-prevent-buying-fake-jeep-trojanbayrob-1

Tips:

- Be cautious about online transactions, especially on neighborhood trading sites and auction sites.
- Be suspicious about any requests to bypass normal trading payment systems or offers to buy goods from completed auctions.
- Check to be sure you can access the auction from other computers or your cell phone. If any requests seem out of order, end the transaction discussion immediately.

A different kind of cybercriminal

Approximately 1 in 7 youth online (10 to 17 years old) received a sexual solicitation or approach over the Internet.[14] Most children report they ignore the message and block the sender. For those less equipped by training or confidence to manage these unwanted come-ons, it's far more serious. While online predation is not statistically as likely to impact your child as other online threats, it is a true cybercrime with very real criminals and victims. And unlike financial cybercrimes, with a predation crime, the victims may never be whole again.

Online predator, Michael Macalindong, was one of the first to move from online chat forums where online predators usually gather to social networking sites. He posed as a young female offering sex in return for sexual favors to be given to a "friend" of the supposed girl. He was convicted of his crimes, which included attempts to blackmail the minor victim.

Another online problem is that of child pornography. The Internet trading and commercialization of horrific sexual imagery involving children has exploded in recent years, despite strong laws and active police efforts to find and punish the sexual offenders who create, receive or traffic the material. The U.S.-based National Center for Missing and Exploited Children (NCMEC) offers a resource for anyone who discovers child pornography online or knows of someone who is seeking to create, acquire, or sell such material. You can report these people to **www.cybertipline.com** or call **1-800- 843-5678** where trained analysts will investigate the report and involve law enforcement in the local jurisdiction.

14. David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. *Online Victimization of Youth: Five Years Later.* Alexandria, Virginia: National Center for Missing & Exploited Children, 2006, pages 7-8, 33.]

Tips:

- Make sure your children know to tell a trusted adult about any online communication that makes them feel uncomfortable.
- Use family safety software, such as **OnlineFamily.Norton**, to help supervise younger children and to monitor who they are in communication with online.
- Discourage or block the use of peer-to-peer file sharing software on your computers that can be used by others to store their images of child pornography. You can be held responsible for any illegal material found on your computers.
- Use strong security settings and software to prevent others from sharing your home network, even a wireless network.
- Make sure you use strong security software such as **Norton Internet Security** to keep your computer and home network safe from criminals who might seek to use your computer to store illegal material.

Protecting yourself from cybercrime

Develop a comprehensive defensive strategy

The burden of stopping the cybercriminal is the responsibility of the individual online computer user. You must construct a comprehensive set of defensive strategies. You'll need an integrated security software suite like those offered by Norton. You'll need to keep your security software, operating system, and browser updated and patched to close any security vulnerabilities. And, perhaps most important, you must be careful about where you go and the choices you make when you're online.

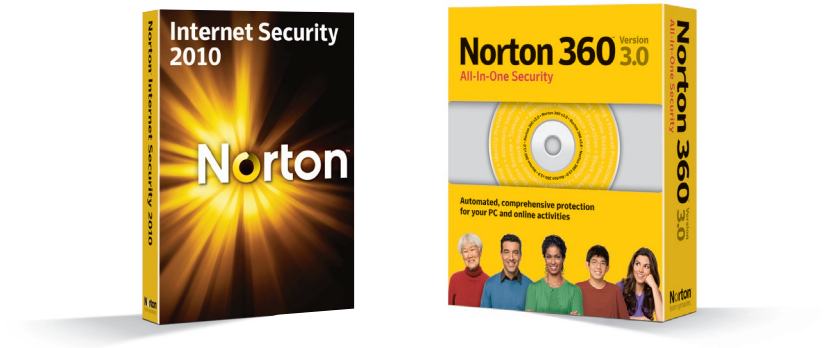
Norton from Symantec, detecting and protecting against cybercrime

At Norton from Symantec, we are dedicated to fighting cybercrime and helping to protect your online experience. We believe you have digital rights, similar to your rights in offline society.

Not only do we develop the world's leading security software—used by 120 million customers worldwide—but we conduct extensive research into the nature and construct of the underground cybercriminal world. This knowledge allows us to provide you with market-leading protection against an ever-changing battleground.

Norton 2010—Defending your digital rights

Norton Internet Security and **Norton 360** give you the power to deny cybercriminal attacks and keep them from wreaking havoc on your family, finances, reputation, and your life. We defend your digital rights to help you have complete control of your online experience.



The right to feel safe

- Parental controls protect your children from online predators and block inappropriate websites based on pre-defined and customizable child, teen, and adult profiles.
- 40,000 security sensors, 4 security operations centers, and intelligence from more than 18 million members of our Norton Community Watch provide you with the best protection against today's online threats.
- Norton Insight uses Symantec's global security intelligence network to provide real-time protection from the newest threats.

The right to your identity

- Norton Identity Safe protects your identity when you shop, bank, and browse online.
- Norton Identity Safe On-The-Go lets you access your most recent log-ins and passwords with a USB drive on any PC protected by Norton Internet Security 2010.
- Phishing scams are intended to trick you into giving usernames and passwords to criminals on phony websites. Norton's advanced protection keeps your personal information safe by blocking known and hard-to-detect phishing sites.

The right to be free from exploitation

- Bot Protection prevents criminals from taking control of your computer, accessing your private information, or using your PC to host an attack.

The right to be aware of dangers

- Norton Safe Search identifies unsafe and dangerous websites right in your search results.
- Norton Safe Web is an online tool that lets you look up a site to see if it's safe.

The right to be free from unnecessary barriers

- Rapid installation gets you up and running quickly with only one mouse click—on average in less than one minute.
- Norton Internet Security 2010 is designed to have little impact on your system's performance and uses an average of less than 7 MB of memory between system scans.
- Norton System Insight lists features and easy-to-understand system information to help keep computers performing at top speed.

Glossary

Black Market/Underground Economy

An efficient, online global marketplace where stolen goods and fraud-related services are regularly bought and sold.

http://www.symantec.com/about/news/release/article.jsp?prid=20081123_01

Black Market Commodities

A variety of commodities traded. Following is a partial list of items considered valuable:

- Credit card numbers—typically CVV2 numbers (3-4 digit numbers on the back of a card) are required as well for these to be considered of any value
- Root or administrative access to servers—hacked servers which the criminals can access at their leisure to host phishing websites—often referred to as "roots" in chat rooms and forums
- Email address lists used either for spam or as targets of phishing scams
- Online banking accounts
- Online payment service accounts
- Counterfeit currency

SOURCE: **http://www.symantec.com/norton/cybercrime/blackmarket.jsp**

Bot or **Botnet**

Short for robot, a bot is a small hidden application that is sent by cybercriminals to unsuspecting computers like yours. It then uses your computer to perpetrate criminal activities such as sending spam emails or phishing attacks. Botnets are networks of bots working together to perpetuate massive attacks in thousands or even millions of computers.

Cybercriminal

A thief that commits crimes via computers, networks or hardware devices.

Cybercrime

Any crime that is committed using a computer, a network, or hardware device. Attacks include keystroke loggers, viruses, rootkits or Trojan horses, phishing, pharming, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud.

SOURCE: **http://www.symantec.com/norton/cybercrime/definition.jsp**

Crimeware

Includes programs that may be classified as bots, keystroke loggers, spyware, backdoors and Trojan horses.

SOURCE: **http://www.symantec.com/norton/cybercrime/definition.jsp**

Hacking

Person or group of people who use unauthorized methods to access a computer or network of computers, usually for illegal purposes.

Keystroke Logger

A simple, readily available spyware application, loaded onto target computers via spam or click fraud Trojans, that records every keystroke on your computer, and sends your information back to the cybercriminal.

Phishing

Spam email that appears to be legitimate but is not. Its goal is to get you to send personal information to the cybercriminal.

Spam

Spam is a catch-all term for any unsolicited email. Much of it is just bothersome correspondence from legitimate businesses. But some of it has criminal intent, whether phishing for information, attempting to load malicious code onto your computer, trying to enlist you in a scam, or trying to seduce children.

Trojan

Trojans are applications sent to your computer, either via spam or click-fraud that sit silently on your computer and download spyware bots or other malicious applications to your computer.

Underground Economy

The underground economy, as it pertains to the Internet, is a massive global market that trades in tools for cybercriminals, as well as the personal financial information of millions of people.

Vulnerability

A weakness or hole in an operating system, browser or network that can be exploited by cybercriminals.

Web-based Attack

Any malicious attack, personal or financial, that originates on the Internet.

CYBERCRIME
EXPOSED

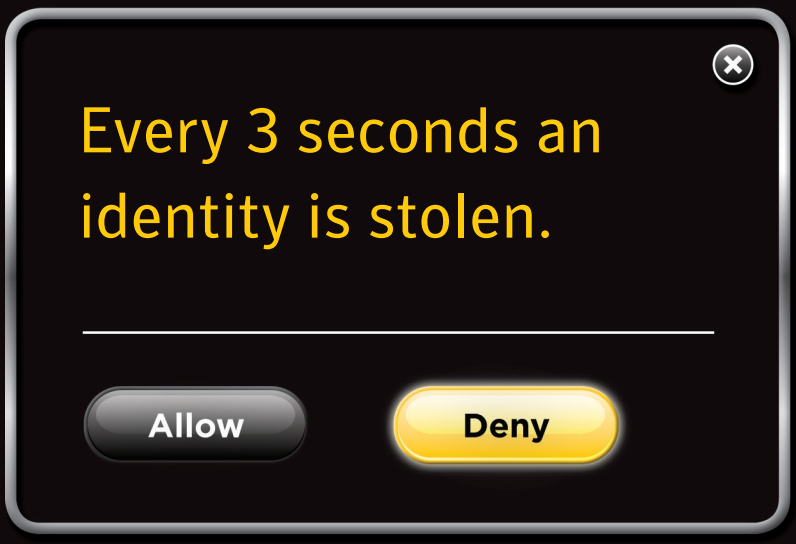
Resources for victims of cybercrime

- Reporting password theft/trafficking
  www.ic3.gov
- Child pornography, child exploitation and online predators
  www.cybertipline.com (NCMEC)
  www.ic3.gov
- Internet fraud and spam
  www.ic3.gov
- ID theft resource center
  www.idtheftcenter.org
- Phishing attacks
  www.us-cert.gov
  www.antiphishing.org
- Reporting stolen credit cards
  contact your credit card issuer (financial institution)
- Credit reporting agencies (where to report fraud)

  Equifax
  800-525-6285
  www.equifax.com

  Experian
  888-397-3742
  www.experian.com
  (or by mail):
  Experian National Consumer Assistance Center
  P.O. Box 9530, Allen, TX 75013

  TransUnion
  800-680-7289
  www.transunion.com



Norton™
from symantec