www.jump2learn.com

Jump2Learn
PUBLICATION

E-COMMERCE & CYBER SECURITY

Jump2Learn - The Online Learning Place

Ms. Sonal B. Shah | Mrs. Krupali P. Patel | Mr. Nitesh G. Patel

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it.

In CRM (customer relationship management), CRM software is a category of software that covers a broad set of applications designed to **help** businesses manage many of the following business processes:

Customer data.
Customer interaction.
Access business information for customer.

Content marketing
A type of marketing that involves the creation and sharing of online material (such as videos, blogs, and social media posts) that does not explicitly promote a brand but is intended to stimulate interest in its products or services.

Forgery
(criminal law) the false making or altering of any document, such as a cheque or character reference (and including a postage stamp), or any tape or disc on which information is stored, intending that anyone shall accept it as genuine and so act to his or another's prejudice.

A **set-top box (STB)** or **set-top unit (STU)** (one type also colloquially known as a cable box) is an information appliance device that generally contains a TV-tuner input and displays output to a television set and an external source of signal, turning the source signal into content in a form that then be displayed on the television screen or other display device. They are used in cable television, satellite television, and over-the-air television systems, as well as other uses.

5.1 Pornography
Printed or visual material containing the explicit description or display of sexual organs or activity, intended to stimulate sexual excitement.
People can get in trouble before they even realize it. When it is so easy to access sexually explicit materials on the Internet, users can find themselves acting on curiosities they didn't have before. Some people find themselves losing control over their use of pornography, for example by spending more and more time viewing it and, for some, looking for new and different types of pornography, including images of children. Some people accidentally find sexual images of children and are curious or

aroused by them. They may justify their behavior by saying they weren't looking for the pictures, they just "stumbled across" them, etc.

How to Avoid Pornography

1. Clean up your computer. Get rid of any porn you have saved.
2. Set up an internet censor.
3. Spend your free time with friends or family.
4. Use positive reinforcement instead of negative.
5. Pick up a new habit or hobby, such as exercising.
6. Seek out counseling if the problem continues.

5.2 IPR Violations:

Software piracy, Copyright Infringement, Trademarks Violations, Theft of Computer source code, Patent Violations:

An **intellectual property infringement** is the infringement or violation of an intellectual property right. There are several types of intellectual property rights, such as copyrights, patents, and trademarks. Therefore, an intellectual property infringement may for instance be a

- Copyright infringement
- Patent infringement
- Trademark infringement

Copyright infringement is the use of works protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works. The copyright holder is typically the work's creator, or a publisher or other business to whom copyright has been assigned. Copyright holders routinely invoke legal and technological measures to prevent and penalize copyright infringement.

Copyright infringement disputes are usually resolved through direct negotiation, a notice and take down process, or litigation in civil court. Egregious or large-scale commercial infringement, especially when it involves counterfeiting, is sometimes prosecuted via the criminal justice system. Shifting public expectations, advances in digital technology, and the increasing reach of the Internet have led to such widespread, anonymous infringement that copyright-dependent industries now focus less on pursuing individuals who seek and share copyright-protected content online, and more on expanding copyright law to recognize and penalize – as "indirect" infringers – the

service providers and software distributors which are said to facilitate and encourage individual acts of infringement by others.

Patent infringement is the commission of a prohibited act with respect to a patented invention without permission from the patent holder. Permission may typically be granted in the form of a license. The definition of patent infringement may vary by jurisdiction, but it typically includes using or selling the patented invention. In many countries, a use is required to be *commercial* (or to have a *commercial* purpose) to constitute patent infringement.

The scope of the patented invention or the extent of protection is defined in the claims of the granted patent. In other words, the terms of the claims inform the public of what is not allowed without the permission of the patent holder.

Patents are territorial, and infringement is only possible in a country where a patent is in force. For example, if a patent is granted in the United States, then anyone in the United States is prohibited from making, using, selling or importing the patented item, while people in other countries may be free to exploit the patented invention in their country. The scope of protection may vary from country to country, because the patent is examined -or in some countries not substantively examined- by the patent office in each country or region and may be subject to different patentability requirements.

Trademark infringement is a violation of the exclusive rights attached to a trademark without the authorization of the trademark owner or any licensees (provided that such authorization was within the scope of the licence). Infringement may occur when one party, the "infringer", uses a trademark which is identical or confusingly similar to a trademark owned by another party, in relation to products or services which are identical or similar to the products or services which the registration covers. An owner of a trademark may commence civil legal proceedings against a party which infringes its registered trademark. In the United States, the Trademark Counterfeiting Act of 1984 criminalized the intentional trade in counterfeit goods and services.

5.3 Cyber Squatting

Cyber squatting refers to illegal domain name registration or use. Cyber squatting can have a few different variations, but its primary purpose is to steal or misspell a domain name in order to profit from an increase in website visits, which otherwise would not be possible. Trademark or copyright holders may neglect to reregister their domain names, and by forgetting this important update, cyber squatters can easily steal domain names. Cyber squatting also includes advertisers who mimic domain names that are similar to

popular, highly trafficked websites. Cyber squatting is one of several types of cybercrimes.

Cyber squatting is also known as domain squatting.

The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization charged with overseeing domain name registration. As Cyber squatting complaints throttle up worldwide, ICANN has implemented thorough standards of acceptance such that domain name assigning is done with much more scrutiny. ICANN has also put solid requirements for domain name recovery in place for instances of trademark registration lapses by trademark owners. ICANN urges trademark owners to renew their registrations yearly and to report misuse to the agency as soon they become aware that they've neglected to reregister a domain.

QR code:

QR codes can be a really easy to use and beneficial tool in the world of retail. A great way to use QR codes in retail is to place a mobile barcode on the tag of every item in the store. This way, potential customers can scan the code and look at product specifications as well as reviews of the product they are interested in buying. While some customers may want a sales associate to walk them through the process of scanning the QR codes, others are familiar with the technology and will want to do it on their own, so make sure customers are given the option.

Another way QR codes are used in retail is by mobilizing online retail sites and using QR codes to drive potential customers to the site to hopefully make a purchase. These QR codes can be placed around towns and cities and can also be placed online on social

media profiles such as Twitter and Facebook. The more the QR code is seen, the more it will be scanned, and the more sales a company will make.

QR Codes are becoming part or everyday life. But more importantly they are becoming a part of business and retail. This medium is building up steam and is on its way to becoming very trendy. More people than ever before are utilizing the powerful informational tool and making it profitable.

Manufacturers used to use QR Codes to track parts, not it can provide a wealth of information to the everyday consumers. More often now it is providing product information. More consumers are being reached with QR Code marketing campaigns.

Consumers can now compare products and prices instantly with technology provided by smart phones with barcode scanner applications. The allure [attraction] of instantly downloadable coupons and discounts is now possible with these QR Codes. And the provocative nature of this technology is reaching audiences that many advertisers did not think was possible.

Retailers and small businesses are now seeing how easy it is to create QR Codes and use them to connect with their client base. Free QR Code generators are everywhere now. And now that we live in an era where having a social media account of some sort is almost mandatory, sharing the QR Codes that carry valuable data for one's potential clients, is becoming easier than ever to share.

Gone are the days of coaxing people into filling out a long form to get them on your mailing list with the promise of occasional deals in regular newsletters. Now it's becoming as quick and point, click, and scan to get a coupon and quickly sign up for a product mailing list. QR Codes have helped the retail industry evolve and their uses become more advanced every day.

Benefits of Using QR Codes for the Customer

Having a mobile website and using QR codes with it can place a positive first impression of your business in the consumer's mind. By incorporating QR codes into any kind of print media you use (business cards, magazine ads, coupons, fliers, signs) your customer doesn't have to dial any numbers or even click anything to get where they want to go (or where you want them to go). They don't have to fumble around for a notebook and pen to write down your URL, phone number or physical address. By making it easy for them to find the information they need, you save them time. These positive first impressions actually do bring people into your store. The numbers are telling: 94% of mobile users look for local information on their smart phones—66% of those people actually visit a business in person or online afterward.

5.4 Banking/ Credit card related crimes

Credit card fraud is a wide-ranging term for theft and fraud committed using or involving a payment card, such as a credit card or debit card, as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft. According to the United States Federal Trade Commission, while the rate of identity theft had been holding steady during the mid 2000s, it increased by 21 percent in 2008. However, credit card fraud, that crime which most people associate with ID theft, decreased as a percentage of all ID theft complaints for the sixth year in a row.

5.5 ecommerce / Investment Frauds

E-commerce fraud is constantly increasing, and alternative payment methods are attracting criminals.

While the increase itself is nothing new (there has been more e-commerce fraud every year since 1993), the rate is impressive.

Fraud is not exclusive to credit card payments. Criminals are becoming more sophisticated in their use of malware to command online banking logins via phones, tablets and computers, using the stolen bank account details to make fraudulent payments.

Identity theft

According to the study, the most common types of e-commerce fraud causing concern among merchants are identity theft (71%), phishing (66%) and account theft (63%). Here, credit cards are the most popular target, as a fraudster does not need much to carry out a 'card not present' transaction.

In traditional identity theft, the criminals' goal is to carry out transactions using a different identity. Instead of having to come up with a completely new identity to do this, they simply take over an existing one. This is easier to do – and usually much faster.

In order to commit identity theft or appropriate someone's identity, fraudsters target personal information, such as names, addresses and email addresses, as well as credit card or account information.

This enables them, for example, to order items online under a false name and pay using someone else's credit card information or by debiting another person's account. Phishing, on the other hand, simply involves using fraudulent websites, emails or text messages to access personal data.

Another technical method is known as pharming, in which manipulated browsers direct unsuspecting customers to fraudulent websites. Often, all that is required to appropriate someone's identity is a stolen password. This can be used to take over an existing account with an online shop – in most cases, the payment data is already stored in the account.

Of course, hacker attacks on e-commerce providers and stealing customer data also fall under this type of e-commerce fraud, as does using malware on computers to commit identity theft by spying out sensitive data.

Friendly fraud

In fourth place is what the merchants surveyed refer to as 'friendly fraud'. This sounds friendlier than it really is: using this method, customers order goods or services and pay for them – preferably using a "pull" payment method like a credit card or direct debit.

Then, however, they deliberately initiate a charge-back, claiming that their credit card or account details were stolen. They are reimbursed – but they keep the goods or services. This fraud method is particularly prevalent with services, such as those in the gambling or adult milieus. Friendly fraud also tends to be combined with re-shipping.

This is where criminals who use stolen payment data to pay for their purchases don't want to have them sent to their home addresses. Instead, they use middlemen whose details are used to make the purchases and who then forward the goods.

Clean fraud

Clean fraud's name is misleading, because there's nothing clean about it. The basic principle of clean fraud is that a stolen credit card is used to make a purchase, but the transaction is then manipulated in such a way that fraud detection functions are circumvented.

Much more know-how is required here than with friendly fraud, where the only goal is to cancel the payment once a purchase has been made. In clean fraud, criminals use sound

analyses of the fraud detection systems deployed, plus a great deal of knowledge about the rightful owners of their stolen credit cards.

A great deal of correct information is then entered during the payment process so that the fraud detection solution is fooled. Before clean fraud is committed, card testing is often carried out. This involves making cheap test purchases online to check that the stolen credit card data works.

Affiliate fraud

There are two variations of affiliate fraud, both of which have the same aim: to glean more money from an affiliate program by manipulating traffic or signup statistics. This can be done either using a fully automated process or by getting real people to log into merchants' sites using fake accounts. This type of fraud is payment-method-neutral, but extremely widely distributed.

Triangulation fraud

During triangulation fraud, the fraud is carried out via three points. The first is a fake online storefront, which offers high-demand goods at extremely low prices. In most cases, additional bait is added, like the information that the goods will only be shipped immediately if the goods are paid for using a credit card. The falsified shop collects address and credit card data – this is its only purpose.

The second corner of the fraud triangle involves using other stolen credit card data and the name collected to order goods at a real store and ship them to the original customer.

5.6 Defamation (Cyber Smearing)

Cyber smearing is the act of anonymous communication of false information about a corporation over the Internet, which causes economic damages. Initially, Internet Service Providers (ISPs) were concerned with their legal liability, which was limited by the Communication Decency Act of 1996.

5.7 Cyber Stacking

Cyberstalking is a criminal practice where an individual uses the Internet to systematically harass or threaten someone. This crime can be perpetrated through email, social media, chat rooms, instant messaging clients and any other online medium. Cyberstalking can also occur in conjunction with the more traditional form of stalking, where the offender harasses the victim offline. There is no unified legal approach to cyberstalking, but many governments have moved toward making these practices punishable by law.

Cyberstalking is sometimes referred to as Internet stalking, e-stalking or online stalking.

Cyberstalking is one of several cybercrimes that have been enabled by the Internet. It overlaps with cyberbullying and cyber luring in that many of the same techniques are used. Social media, blogs, photo sharing sites and many other commonly used online sharing activities provide Cyberstalkers with a wealth of information that helps them plan their harassment. By collecting personal data (profile pages) and making notes of frequented locations (photo tags, blog posts), the cyberstalker can begin to keeping tabs on an individual's daily life.

The National Center for Victims of Crime (NCVC) suggests that victims of cyberstalking take the following steps:

- For minors, inform parents or a trusted adult
- File a complaint with the cyberstalker's Internet service provider
- Collect evidence, document instances and create a log of attempts to stop the harassment
- Present documentation to local law enforcement and explore legal avenues
- Get a new email address and increase privacy settings on public sites
- Purchase privacy protection software
- Request removal from online directories

Definition of Cyber Terrorism

The Federal Bureau of Investigation (FBI) enforces federal laws, those created by Congress which applies to everyone nationwide. One area of law which they enforce is **cyber terrorism**, which involves crimes of terrorism that occur electronically. These crimes occur against individuals, businesses, organizations, and against the government itself.

So much of our lives are accessible electronically now - from your social security number on a job application, to your bank account, to medical records and more. With the greater convenience of using technology, we trade off some degree of security since it's very difficult to stop every instance of cyber terrorism. Consider for a moment, how much of your own private information could a hacker potentially find online about your life? Who or what protects you against theft or other crimes related to your personal data?

Cyber terrorism is a phrase used to describe the use of Internet based attacks in **terrorist** activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses.

Examples of cyber terrorism

Acts of cyber terrorism can be carried out over private computer servers, against devices and networks visible through the public internet as well as against secured government networks or other restricted networks. Hackers who break into computer systems can introduce viruses to vulnerable networks, deface websites, launch denial-of-service attacks and/or make terroristic threats electronically.

Examples of cyber terrorism include:

- Global terror networks disrupting major websites to create public nuisances/inconveniences or to stop traffic to websites that publish content the hackers disagree with.
- International cyber terrorists accessing and disabling or modifying the signals that control military technology.
- Cyber terrorists targeting critical infrastructure systems, for example, to disable a water treatment plant, cause a regional power outage, or disrupt a pipeline, oil refinery or franking operation. This type of cyber-attack could disrupt major cities, cause a public health crisis, endanger the public safety of millions of people as well as cause massive panic and fatalities.

Cyber espionage, as carried out by governments using hackers to spy on rival nations' intelligence communications to learn about the locations of troops or gain a tactical advantage at war, is not necessarily considered to be cyber terrorism unless the spying is carried out with the intent to execute a cyber-terrorist attack.