Abstract this paper gives a detailed information

Art & Culture, Music

AbstractWe live in an era ofcomputer technology which is running by cyber network where we can get anyinformation by just clicking or typing.

With the updating of technology cybercrimeis also increasing in all the sectors. Cybercrime is a such kind of activity inwhere some technologically advanced people stealing others valuable data anddocuments, hacking bank account, creating malware/virus and spreading them, bombing mail, spreading spam messages and phishing sites and so on. It isnecessary to prevent the cybercrime and fight back to these types of culpritsto save the people. Where we here the term “ Cybercrime” our focus is gone on” Cyber security”. This paper gives a detailed information all about cybercrimeand its properties and how can we prevent cybercrime and control its internalsecurity.

Introduction : The advantages of technology and the internet haveled more criminals to use cyberspace to commit crimes. The threat of cybercrimeis increasing as globalization continues to spread across the world. While theimpact of globalization has led to amazing, new discoveries throughout theworld, Internet connectivity has also made cybercrime easier.

America and therest of the world have become more reliant on technology and use it in moreaspects of their lives, technology-users make themselves more vulnerable tocyber attacks. Globalization and the growing use of computers in the world havegiven people a motive to learn more about computing and become moreknowledgeable as programmers. As these people learn more, there is a risk thatthey will use their new intelligence to commit cybercrimes. Definition of cyber crime:” Cyber crime” means any

criminal or other offencethat is facilitated by or involves the use of electronic communications orinformation systems, including any device or the Internet or any one or more ofthem. Moreover Cybercrime encompasses criminal actions that target computer, internet, or network utility, damaging functionality or infiltrating systemsand processes. Why do people commit computer crimes? 1. Forfinancial gainCriminal gangs are well-organized and operate on acommercial basis – there is a supply chain, those that steal data are unlikelyto be the same criminals who commit the identity theft and fraud.

The dark webprovides a market place for stolen credentials – with those that have stolenpersonal data selling it on to those who wish to commit fraud. Cyber-attacks with financial demands. A moderntake on blackmail, this can affect organizations of all sizes as well asindividuals.

There are many variations — for example, hackers takeover avictim’s computer and freeze it, they then offer to reinstate access after aransom has been paid. Another variation lead to a recent case where guests at ahotel in Austria were prevented from entering their rooms until a ransom hadbeen paid – the hotel is reportedly removing electronic locks accessed withcards and reverting to old-fashioned keys! 2. Tomake a political or social pointHacktivism involves breaking into a system forpolitical or social reasons.

Until relatively recently, this was seen as thedomain of underground organizations such as Anonymous. The recent US electionhas put focus on the role that governments might play in furthering their aimsthrough hacking

activity. Many businesses may feel that they are unlikely to bea target for political or social hactivists, though it is well to be aware thatthe targets of these attacks vary greatly.

If someone objects to youroperations, you could find yourself at the wrong end of a hacktivist attack. 3. Forthe intellectual challengeThis type of hacker plays to the stereotype of thesocially awkward loner who lives in a virtual world and turns to hacking forboth the intellectual challenge and the adrenaline rush of breaking into anetwork.

Those who hack for intellectual stimulation are notnecessarily criminals. They could be “ white hat” hackers who help organizationsto explore their vulnerabilities so that they can put defenses in place. While white hat hackers work with or for companiesand are a force for good, other hackers motivated by intellectual challenge cancause harm.

While they may not have bad intentions hackers, particularly theinexperienced who are often referred to as ‘ script kiddies’ can cause damageduring their incursions and leave systems vulnerable to those with ill intent. Categorization of Cyber CrimeCyber crimes are broadly categorized into threecategories, namely crime against1. Individual2. Property3. GovernmentEach category can use a variety of methods and themethods used vary from one criminal to another. Individual: Thistype of cyber crime can be in the form of cyber stalking, distributingpornography, trafficking and “ grooming”. Today, law enforcement agencies aretaking this category of cyber crime very seriously and are joining forcesinternationally to reach and arrest the perpetrators. Property: Justlike in the real world

where a criminal can steal and rob, even in the cyberworld criminals resort to stealing and robbing.

In this case, they can steal aperson’s bank details and siphon off money; misuse the credit card to makenumerous purchases online; run a scam to get naïve people to part with theirhard earned money; use malicious software to gain access to an organization’swebsite or disrupt the systems of the organization. The malicious software canalso damage software and hardware, just like vandals damage property in theoffline world. Government: Althoughnot as common as the other two categories, crimes against a government arereferred to as cyber terrorism.

If successful, this category can wreak havocand cause panic amongst the civilian population. In this category, criminalshack government websites, military websites or circulate propaganda. Theperpetrators can be terrorist outfits or unfriendly governments of othernations. How criminals do it? When any crime is committed over the Internet it isreferred to as a cyber crime. There are many way to do cyber crimes and themost common ones are explained below: Hacking: Thisis a type of crime wherein a person’s computer is broken into so that hispersonal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is differentfrom ethical hacking, which many organizations use to check their Internetsecurity protection. In hacking, the criminal uses a variety of software toenter a person’s computer and the person may not be aware that his computer isbeing accessed from a remote location.

Theft: Thiscrime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encouragesoftware piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are lawsthat prevent people from illegal downloading.

CyberStalking: This is a kind of online harassment whereinthe victim is subjected to a barrage of online messages and emails. Typically, these stalkers know their victims and instead of resorting to offline stalking, they use the Internet to stalk. However, if they notice that cyber stalking isnot having the desired effect, they begin offline stalking along with cyberstalking to make the victims' lives more miserable.

IdentityTheft: This has become a major problem with peopleusing the Internet for cash transactions and banking services. In this cybercrime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money orto buy things online in the victim's name. It can result in major financiallosses for the victim and even spoil the victim's credit history.

MaliciousSoftware: These are Internet-based software or programsthat are used to disrupt a network. The software is used to gain access to asystem to steal sensitive information or data or causing damage to softwarepresent in the system.

ComputerViruses: Computer viruses are computer programs that, when opened, put copies of themselves into other computers' hard drives withoutthe users' consent. Creating a computer virus and disseminating it is

a cybercrime. The virus may steal disk space, access personal information, ruin dataon the computer or send information out to the other computer user’s personalcontacts. The most common way for avirus to infect a computer is by way of an email attachment. Effects of Cyber CrimeCriminals take advantage of technology in manydifferent ways.

The Internet, in particular, is a great tool for scammers andother miscreants, since it allows them to ply their trade while hiding behind ashield of digital anonymity. Cyber crime affects society in a number ofdifferent ways, both online and in the offline world. IdentityTheftBecoming the victim of cyber crime can have long-lastingeffects on your life. One common technique scammers employ is phishing, sendingfalse emails purporting to come from a bank or other financial institutionrequesting personal information.

If you hand over this information, it canallow the criminal to access your bank and credit accounts, as well as open newaccounts and destroy your credit rating. This type of damage can take months oreven years to fix, so protecting your personal information online is animportant skill to learn. SecurityCostsCyber criminals also focus their attacks onbusinesses, both large and small. Hackers may attempt to take over companyservers to steal information or use the machines for their own purposes, requiring companies to hire staff and update software to keep intruders out. According to EWeek, a survey of large companies found an average expenditure of$8. 9 million per year on cyber security, with 100 percent of firms surveyedreporting at least one malware incident in the preceding 12 months and 71percent reporting the hijacking of company computers by outsiders.

MonetaryLossesThe overall monetary losses from cyber crime can beimmense. According to a 2012 report by Symantec, more than 1.

5 million peoplefall victim to some sort of cyber crime every day, ranging from simple passwordtheft to extensive monetary swindles. With an average loss of $197 per victim, this adds up to more than $110 billion dollars lost to cyber crime worldwideevery year. As consumers get wise to traditional avenues of attack, cyber criminalshave developed new techniques involving mobile devices and social networks tokeep their illicit gains flowing. PiracyThe cyber crime of piracy has had major effects onthe entertainment, music and software industries. Claims of damages are hard toestimate and even harder to verify, with estimates ranging widely from hundredsof millions to hundreds of billions of dollars per year.

In response, copyrightholders have lobbied for stricter laws against intellectual property theft, resulting in laws like the Digital Millennium Copyright Act. These laws allowcopyright holders to target file sharers and sue them for large sums of moneyto counteract the financial damage of their activities online. What Should We Do? Training and awareness are important first steps in mitigating these attacks. All citizens, consumers, and employees should be aware of cyber threats and theactions they can take to protect their own information, as well as theinformation within their organization. So, what can you do to minimize the riskof becoming a cyber crime victim? 1. Usestrong passwords: Use separate ID/password combinationsfor different accounts and avoid writing them down. Make the

passwords morecomplicated by combining letters, numbers, special characters, and by changingpasswords on a regular basis. 2.

Enableyour firewall: Firewalls are the first line of cyberdefense; they block connections from suspicious traffic and will keep out sometypes of viruses and hackers. 3. Useanti-virus/malware software: Prevent viruses from infectingyour computer by installing and regularly updating anti-virus software. 4.

Blockspyware attacks: Prevent spyware from infiltrating yourcomputer by installing and updating anti-spyware software. 5. Secureyour mobile devices: Be aware that your mobile device isvulnerable to viruses and hackers. Download applications from trusted sources. Do not store unnecessary or sensitive information on your mobile device.

It isalso important to keep the device physically secure; millions of mobile devicesare lost each year. If you do lose your device, it should immediately bereported to your carrier and/or organization. There are some devices that allowremote erasing of data. Be sure to keep your mobile device password protected. 6.

Installthe latest operating system updates: Keep yourapplications and operating system (for example: Microsoft® Windows®, Apple®Mac, and Linux) current with the latest system updates. Turn on automaticupdates to prevent potential attacks on older software. 7. Protectyour data: Use encryption for your most sensitive files, suchas health records, tax returns, and financial records.

Make regular back-ups ofall your important data. 8. Secureyour wireless network: Wi-Fi (wireless) networks at homeare vulnerable to intrusion if they are not properly secured. Review and modifydefault settings. Public Wi-Fi, also known as “ hot spots,” may be vulnerable. Avoid conducting sensitive transactions on these networks. 9.

Protectyour e-identity: Be cautious when giving out personalinformation, such as your name, address, telephone number, or financialinformation on the Internet. Make sure that websites are secure, especiallywhen making online purchases, or that you have enabled privacy settings (forexample: when accessing/using social networking sites, such as Facebook, Twitter®, YouTube, etc.). Once something is posted on the Internet, it may bethere forever. 10. Avoid being scammed: Never reply to emails that ask you to verify your information or confirm youruser ID or password. Don’t click on a link or file of unknown origin.

Check thesource of the message; when in doubt, verify the source. Conclusion: Though not all people are victims to cyber crimes, they are still at risk. Crimes by computer vary, and they don’t always occurbehind the computer, but they executed by computer. The hacker could live threecontinents away from its victim, and they wouldn’t even know they were beinghacked. Crimes done behind the computer are the 21st century’s problem. Withthe technology increasing, criminals don’t have to rob banks, nor do they haveto be outside in order to commit any crime. They have everything they need ontheir lap.

Their weapons aren’t guns anymore; they attack with mouse cursorsand passwords.