Dr. Kailash Bhargava & Dr. Renu Bhargava

HACKING COMPUTER AND BLACKMAILING: ABUSE OF INTERNET

[1]Dr. Kailash Bhargava & [2]Dr. Renu Bhargava

[1]Retd. Professor, Deptt. of Chemistry, DBS College, Kanpur (U P)

[2]Director, Sai Institute of Advanced Studies, Kanpur (UP)

ABSTRACT

Hacking a computer and using stolen data or media to blackmail someone is a serious cybercrime involving unauthorized network access and digital extortion. [1, 2, 3]

What Happens in Hacking & Blackmailing

- Unauthorized Access: Hackers break into personal devices, email accounts, or social media profiles through malware, phishing links, or password breaches. [1, 2, 3]
- Data Theft & Sextortion: They steal private photos, videos, financial documents, or messages, and then threaten to leak them publicly or send them to family and coworkers unless you pay money or meet demands. [1, 2, 3]
- Digital Arrest & Scams: Scammers sometimes impersonate law enforcement officials online, claiming you are under a "digital arrest" to extort money. Note that "digital arrest" is legally non-existent in India. [1]

What to Do If You Are a Victim

- Do Not Pay: Paying rarely stops the blackmailers; they often make repeated demands. [1]
- Preserve Evidence: Take screenshots of the messages, profile IDs, phone numbers, or payment requests before blocking anyone. [1]
- Call National Helpline: Dial 1930 immediately to report financial fraud or cybercrime in India. [1]
- Register a Complaint Online: File an official report at the government cybercrime portal: Cyber Crime Reporting Portal. [1]
- Secure Your Accounts: Change your passwords, enable two-factor authentication (2FA), and run a security scan on your device. [1, 2]

KEYWORDS-hacking, internet,sextortion, blackmailing, abuse

INTRODUCTION

While breaching privacy to detect cybercrime works well when the crimes involve the theft and misuse of information, ranging from credit card numbers and personal data to file sharing of various commodities—music, video, or child pornography—what of crimes that attempt to wreak havoc on the very workings of the machines that make up the network? The story of hacking actually goes back to the 1950s, when a group of phreaks (short for “phone freaks”) began to hijack portions of the world’s telephone networks, making unauthorized long-distance calls and setting up special “party lines” for fellow phreaks. With the proliferation of computer bulletin board systems (BBSs) in the late 1970s, the informal phreaking culture began to coalesce into quasi-organized groups of individuals who graduated from the telephone network to “hacking” corporate and government computer network systems.

Although the term hacker predates computers and was used as early as the mid-1950s in connection with electronic hobbyists, the first recorded instance of its use in connection with computer programmers who were adept at writing, or "hacking," computer code seems to have been in a 1963 article in a student newspaper at the Massachusetts Institute of Technology (MIT). After the first computer systems were linked to multiple users through telephone lines in the early 1960s, hacker came to refer to individuals who gained unauthorized access to computer networks, whether from another computer network or, as personal computers became available, from their own computer systems. Although it is outside the scope of this article to discuss hacker culture, most hackers have not been criminals in the sense of being vandals or of seeking illicit financial rewards. Instead, most have been young people driven by intellectual curiosity; many of these people have gone on to become computer security architects. However, as some hackers sought notoriety among their peers, their exploits led to clear-cut crimes. In particular, hackers began breaking into computer systems and then bragging to one another about their exploits, sharing pilfered documents as trophies to prove their boasts. These exploits grew as hackers not only broke into but sometimes took control of government and corporate computer networks.[1,2,3]

One such criminal was Kevin Mitnick, the first hacker to make the "most wanted list" of the U.S. Federal Bureau of Investigation (FBI). He allegedly broke into the North American Aerospace Defense Command (NORAD) computer in 1981, when he was 17 years old, a feat that brought to the fore the gravity of the threat posed by such security breaches. Concern with hacking contributed first to an overhaul of federal sentencing in the United States, with the 1984 Comprehensive Crime Control Act and then with the Computer Fraud and Abuse Act of 1986.

The scale of hacking crimes is among the most difficult to assess because the victims often prefer not to report the crimes—sometimes out of embarrassment or fear of further security breaches. Officials estimate, however, that hacking costs the world economy billions of dollars annually. Hacking is not always an outside job—a related criminal endeavour involves individuals within corporations or government bureaucracies deliberately altering database records for either profit or political objectives. The greatest losses stem from the theft of proprietary information, sometimes followed up by the extortion of money from the original owner for the data's return. In this sense, hacking is old-fashioned industrial espionage by other means.

One of the largest known case of computer hacking was discovered in late March 2009. It involved government and private computers in at least 103 countries. The worldwide spy network known as GhostNet was discovered by researchers at the University of Toronto, who had been asked by representatives of the Dalai Lama to investigate the exiled Tibetan leader's computers for possible malware. In addition to finding out that the Dalai Lama's computers were compromised, the researchers discovered that GhostNet had infiltrated more than a thousand computers around the world. The highest concentration of compromised systems were within embassies and foreign affairs bureaus of or located in South Asian and Southeast Asian countries. Reportedly, the computers were infected by users who opened e-mail attachments or clicked on Web page links. Once infected with the GhostNet malware, the computers began "phishing" for files throughout the local network—even turning on cameras and video-recording devices for remote monitoring.[4,5,6] Three control servers that ran the malware were located in

Hainan, Guangdong, and Sichuan provinces in China, and a fourth server was located in California.

Computer viruses

The deliberate release of damaging computer viruses is yet another type of cybercrime. In fact, this was the crime of choice of the first person to be convicted in the United States under the Computer Fraud and Abuse Act of 1986. On November 2, 1988, a computer science student at Cornell University named Robert Morris released a software "worm" onto the Internet from MIT (as a guest on the campus, he hoped to remain anonymous). The worm was an experimental self-propagating and replicating computer program that took advantage of flaws in certain e-mail protocols. Due to a mistake in its programming, rather than just sending copies of itself to other computers, this software kept replicating itself on each infected system, filling all the available computer memory. Before a fix was found, the worm had brought some 6,000 computers (one-tenth of the Internet) to a halt. Although Morris's worm cost time and millions of dollars to fix, the event had few commercial consequences, for the Internet had not yet become a fixture of economic affairs. That Morris's father was the head of computer security for the U.S. National Security Agency led the press to treat the event more as a high-tech Oedipal drama than as a foreshadowing of things to come. Since then, ever more harmful viruses have been cooked up by anarchists and misfits from locations as diverse as the United States, Bulgaria, Pakistan, and the Philippines.

Denial of service attacks

Compare the Morris worm with the events of the week of February 7, 2000, when "mafiaboy," a 15-year-old Canadian hacker, orchestrated a series of denial of service attacks (DoS) against several e-commerce sites, including Amazon.com and eBay.com. These attacks used computers at multiple locations to overwhelm the vendors' computers and shut down their World Wide Web (WWW) sites to legitimate commercial traffic. The attacks crippled Internet commerce, with the FBI estimating that the affected sites suffered $1.7 billion in damages. In 1988 the Internet played a role only in the lives of researchers and academics; by 2000 it had become essential to the workings of the U.S. government and economy. Cybercrime had moved from being an issue of individual wrongdoing to being a matter of national security.[7,8,9]

Distributed DoS attacks are a special kind of hacking. A criminal salts an array of computers with computer programs that can be triggered by an external computer user. These programs are known as Trojan horses since they enter the unknowing users' computers as something benign, such as a photo or document attached to an e-mail. At a predesignated time, this Trojan horse program begins to send messages to a predetermined site. If enough computers have been compromised, it is likely that the selected site can be tied up so effectively that little if any legitimate traffic can reach it. One important insight offered by these events has been that much software is insecure, making it easy for even an unskilled hacker to compromise a vast number of machines. Although software companies regularly offer patches to fix software vulnerabilities, not all users implement the updates, and their computers remain vulnerable to criminals wanting to launch DoS attacks. In 2003 the Internet service provider PSINet Europe connected an unprotected server to the Internet. Within 24 hours the server had been attacked 467 times, and after three weeks more than 600 attacks had been recorded. Only vigorous security regimes can protect against such an environment. Despite the claims about the pacific nature of the Internet, it

is best to think of it as a modern example of the Wild West of American lore—with the sheriff far away.

Spam, steganography, and e-mail hacking

E-mail has spawned one of the most significant forms of cybercrime—spam, or unsolicited advertisements for products and services, which experts estimate to comprise roughly 50 percent of the e-mail circulating on the Internet. Spam is a crime against all users of the Internet since it wastes both the storage and network capacities of ISPs, as well as often simply being offensive. Yet, despite various attempts to legislate it out of existence, it remains unclear how spam can be eliminated without violating the freedom of speech in a liberal democratic polity. Unlike junk mail, which has a postage cost associated with it, spam is nearly free for perpetrators—it typically costs the same to send 10 messages as it does to send 10 million.

One of the most significant problems in shutting down spammers involves their use of other individuals' personal computers. Typically, numerous machines connected to the Internet are first infected with a virus or Trojan horse that gives the spammer secret control. Such machines are known as zombie computers, and networks of them, often involving thousands of infected computers, can be activated to flood the Internet with spam or to institute DoS attacks. While the former may be almost benign, including solicitations to purchase legitimate goods, DoS attacks have been deployed in efforts to blackmail Web sites by threatening to shut them down. Cyberexperts estimate that the United States accounts for about one-fourth of the 4–8 million zombie computers in the world and is the origin of nearly one-third of all spam.[10,11,12]

E-mail also serves as an instrument for both traditional criminals and terrorists. While libertarians laud the use of cryptography to ensure privacy in communications, criminals and terrorists may also use cryptographic means to conceal their plans. Law-enforcement officials report that some terrorist groups embed instructions and information in images via a process known as steganography, a sophisticated method of hiding information in plain sight. Even recognizing that something is concealed in this fashion often requires considerable amounts of computing power; actually decoding the information is nearly impossible if one does not have the key to separate the hidden data.

In a type of scam called business e-mail compromise (BEC), an e-mail sent to a business appears to be from an executive at another company with which the business is working. In the e-mail, the "executive" asks for money to be transferred into a certain account. The FBI has estimated that BEC scams have cost American businesses about $750 million.

Sometimes e-mail that an organization would wish to keep secret is obtained and released. In 2014 hackers calling themselves "Guardians of Peace" released e-mail from executives at the motion picture company Sony Pictures Entertainment, as well as other confidential company information. The hackers demanded that Sony Pictures not release The Interview, a comedy about a CIA plot to assassinate North Korean leader Kim Jong-Un, and threatened to attack theatres that showed the movie. After American movie theatre chains canceled screenings, Sony released the movie online and in limited theatrical release. E-mail hacking has even affected politics. In 2016, e-mail at the Democratic National Committee (DNC) was obtained by hackers believed to be in Russia. Just before the Democratic National Convention, the media

organization WikiLeaks released the e-mail, which showed a marked preference of DNC officials for the presidential campaign of Hillary Clinton over that of her challenger Bernie Sanders. DNC chairperson Debbie Wasserman Schultz resigned, and some American commentators speculated that the release of the e-mail showed the preference of the Russian government for Republican nominee Donald Trump.

Sabotage

Another type of hacking involves the hijacking of a government or corporation Web site. Sometimes these crimes have been committed in protest over the incarceration of other hackers; in 1996 the Web site of the U.S. Central Intelligence Agency (CIA) was altered by Swedish hackers to gain international support for their protest of the Swedish government's prosecution of local hackers, and in 1998 the New York Times's Web site was hacked by supporters of the incarcerated hacker Kevin Mitnick. Still other hackers have used their skills to engage in political protests: in 1998 a group calling itself the Legion of the Underground declared "cyberwar" on China and Iraq in protest of alleged human rights abuses and a program to build weapons of mass destruction, respectively. In 2007, Estonian government Web sites, as well as those for banks and the media, were attacked. Russian hackers were suspected because Estonia was then in a dispute with Russia over the removal of a Soviet war memorial in Tallinn.

Sometimes a user's or organization's computer system is attacked and encrypted until a ransom is paid. The software used in such attacks has been dubbed ransomware. The ransom usually demanded is payment in a form of virtual currency, such as Bitcoin. When data are of vital importance to an organization, sometimes the ransom is paid. In 2016 several American hospitals were hit with ransomware attacks, and one hospital paid over $17,000 for its systems to be released.[13,14,15]

Defacing Web sites is a minor matter, though, when compared with the specter of cyberterrorists using the Internet to attack the infrastructure of a nation, by rerouting airline traffic, contaminating the water supply, or disabling nuclear plant safeguards. One consequence of the September 11 attacks on New York City was the destruction of a major telephone and Internet switching centre. Lower Manhattan was effectively cut off from the rest of the world, save for radios and cellular telephones. Since that day, there has been no other attempt to destroy the infrastructure that produces what has been called that "consensual hallucination," cyberspace. Large-scale cyberwar (or "information warfare") has yet to take place, whether initiated by rogue states or terrorist organizations, although both writers and policy makers have imagined it in all too great detail.

In late March 2007 the Idaho National Laboratory released a video demonstrating what catastrophic damage could result from utility systems being compromised by hackers. Several utilities responded by giving the U.S. government permission to run an audit on their systems. In March 2009 the results began to leak out with a report in The Wall Street Journal. In particular, the report indicated that hackers had installed software in some computers that would have enabled them to disrupt electrical services. Homeland Security spokeswoman Amy Kudwa affirmed that no disruptions had occurred, though further audits of electric, water, sewage, and other utilities would continue.

DISCUSSION

Advances in cyberspace technology deeply entangle individuals and entities across nations: its governments, industries, organizations, and academia (NGIOA). While cyberspace brings us a new ecosystem, our individual and collective dependency on cyberspace technology, also brings us critical security risks that are proving extremely difficult to eliminate.

With the advances in science and technology, cyber-crime and blackmail are evolving. As society continues to evolve and technology marches forward, connecting cyberspace to geospace and space, our understanding of the origins of criminality and blackmail also evolves and must be continuously revised. Therefore, the persistence, prevalence, and seriousness of cyber-crime and blackmail offending demands a greater response from not only the security community but from everyone across nations.
It is believed that if you can imagine a form of theft, fraud, or exploitation, it is probably now being perpetrated or abetted by a computer. As a result, it is important to understand what kind of acts in cyberspace are classified as cyber-crimes and what constitutes blackmail and who is the target.[16,17,18]

Why is it important to understand Cyber Blackmail?
Today, because of cyberspace, any form of theft, fraud, or exploitation can probably be perpetrated, programmed, or backed by a computer. As a result, today and every day, millions of people worldwide are being victimized by some sort of computer crime. Moreover, as everything gets digitized, and it becomes increasingly easier to share every aspect of our lives on social media, the probability of private matters getting into the hands of criminals and bad people with bad intentions is increasing rapidly. As a result, cyber-blackmail is on the rise across nations. Cyber intrusions, cyber-crimes, and cyber blackmail are becoming more commonplace, more dangerous, and more sophisticated. Moreover, the ease with which cyber-crime and cyber blackmail cross national borders, and the deceptions that are employed by cybercriminals, obstruct their identification and attribution in cyberspace and geospace. To add to the complexities, the lack of standards and conflicting legal frameworks from across nations prevents cyber-crime forces from identifying and interrogating cyber-crime suspects and catching them in a timely manner.
When the growing cyber-crimes include blackmail that involves harassment, malicious mischief, manipulation, abuse, extortion and so much more, it is understandably becoming a cause of great concern.

RESULTS

Extra Steps To Stay Secure From Hacker Attacks
The best strategy to avoid potential hackers is taking preventative measures before threats arise. There are ways to be proactive with your online safety, and you should take into account the following suggestions to avoid being hacked and blackmailed.

Be Wary of Suspicious Links and Attachments: Avoid clicking on unfamiliar links or opening attachments from unknown sources, as they could contain malware.
Use Strong Passwords: Create complex and unique passwords to lower the risk of your social media and other online accounts being hacked. Consider using a password manager to store and generate passwords securely.

Enable Two-Factor Authentication (2FA): Add an extra layer of security by enabling 2FA on your accounts whenever possible.
Regularly Back Up Data: Keep copies of essential files and documents on an external hard drive or cloud storage service. Regular backups help mitigate the impact of ransomware attacks.
Beware of Phishing Scams: Be cautious of emails or messages asking for personal information. Verify the sender's identity before sharing sensitive data.
Update Privacy Settings: Review and manage privacy settings on social media and other online platforms to limit the amount of personal information available to potential hackers.
Avoid Oversharing: This includes information that is shared both publicly and in private conversations. Disclosing private information online makes you more susceptible to sextortion and other cybercrimes.
Hacking attempts commonly target businesses. Scammers know how crucial it is for companies to protect trade secrets, client information, and other confidential data. If they can gain access, they can threaten to leak, encrypt, or destroy these files unless their demands are met.

While it's well known that businesses need to protect their data, many are still struggling to do so. Whether it's a lack of understanding or willful negligence, here are five common errors that our investigators encounter when handling corporate cyber incidents.[17,18,19]

Lack of cybersecurity knowledge. In order to protect against cyber threats effectively, you need to understand the types of attacks, methods used, and weak points commonly targeted by hackers.
Failure to handle cyber threats seriously. Many companies fail to allocate the time and resources to properly configure their digital security, whether it's to shortcut costs or because it's not viewed as a priority.
Absence of a comprehensive cybersecurity strategy. Without a cohesive plan, security measures are often reactive rather than proactive. A robust cybersecurity strategy ensures that all layers of the organization are aligned to identify, protect, detect, and respond to threats before they escalate.
Improper risk assessment. Even when companies spend the necessary funds on cybersecurity, they may fail to correctly evaluate the threat. This is often the result of a misguided belief that their network is secure.
Insufficient technology. A business may make an initial investment towards their cyber protection and wrongly believe they will stay secure. However, cyber threats are constantly evolving, and security systems need to keep pace.
Human error. The largest vulnerability in a company's cyber security is people. Inadequate staff training can lead to misconfigured remote devices, phishing attacks, and unconcealed credentials that can open the door for a threat actor.

CONCLUSIONS

Some sensible tips to protect your organization and personal data from cybercrimes include:

Regularly update your operating systems, devices, software, and websites with the latest patches to safeguard your data. Enable automatic updates whenever feasible.

Using anti-virus software like Kaspersky Premium, Avast One, McAfee+ Premium, and Avira Internet Security is a great way to protect your system from attacks. Anti-virus software allows you to detect and remove threats before they become a problem.

Stay informed about current cyber threats and trends and adapt security measures accordingly. If you are an employer, conduct regular cybersecurity training sessions for employees about the best cybersecurity practices.

Create strong passwords that are difficult to guess using a mix of letters, numbers, and special characters. Avoid easy-to-guess passwords like birthdays or common words. Implement two-factor authentication whenever possible to add an extra layer of security.

Never open attachments in spam emails, as this is a classic way to infect your computer. Exercise caution when clicking links or downloading email attachments, especially from unknown or suspicious sources.

Never give out personal information over the phone or via email unless you're entirely sure the line or email is safe. Make sure that you're speaking to the person you think you are.

Be mindful of which website URLs you visit. Avoid clicking on links with unfamiliar URLs that look like spam. If your internet security product includes functionality to secure online transactions, enable it before conducting financial transactions online.

Secure your data by regularly backing up information. Effective data protection measures like off-site backups, encryption, and secure cloud storage are critical against cyber threats like ransomware that could steal, damage, or destroy your data.[20]

REFERENCES

1. Sukhai, Nataliya B. (8 October 2004). "Hacking and cybercrime". Proceedings of the 1st annual conference on Information security curriculum development. New York, United States: ACM. pp. 128–132. doi:10.1145/1059524.1059553. ISBN 978-1-59593-048-4. S2CID 46562809. Archived from the original on 18 July 2024. Retrieved 10 December 2023.
2. Rassolov, I. M. (2025). Информационное право [Information Law] (in Russian) (7th ed.). Retrieved 8 August 2025 – via Образовательная платформа «Юрайт».
3. "BUFFETT: This is 'the number one problem with mankind'". Business Insider. Archived from the original on 9 June 2023. Retrieved 17 May 2021.
4. "Warren Buffett: 'Cyber poses real risks to humanity'". finance.yahoo.com. 30 April 2019. Archived from the original on 2 June 2023. Retrieved 17 May 2021.
5. "The Global Risk Report 2020" (PDF). World Economic Forum. 15th Edition: 102. 15 January 2020. Archived (PDF) from the original on 27 September 2023. Retrieved 17 May 2021.
6. Heading, Sophie; Zahidi, Saadia (January 2023). "The Global Risks Report 2023, 18th Edition" (PDF). World Economic Forum. Archived (PDF) from the original on 5 February 2024. Retrieved 3 February 2024.
7. "Law and the Internet: Theoretical Problems". Retrieved 20 November 2024.

8. Gordon, Sarah (25 July 2006). "On the definition and classification of cybercrime". Journal in Computer Virology. 2: 13–20. doi:10.1007/s11416-006-0015-z. S2CID 3334277.
9. Richet, Jean-Loup (1 January 2022). "How cybercriminal communities grow and change: An investigation of ad-fraud communities". Technological Forecasting and Social Change. 174 (121282) 121282. doi:10.1016/j.techfore.2021.121282. ISSN 0040-1625. S2CID 239962449.
10. Chandra, Akhilesh; Snowe, Melissa J. (1 September 2020). "A taxonomy of cybercrime: Theory and design". International Journal of Accounting Information Systems. 2019 UW CISA Symposium. 38 100467. doi:10.1016/j.accinf.2020.100467. ISSN 1467-0895.
11. Lehman, Jeffrey; Phelps, Shirelle (2005). West's Encyclopedia of American Law, Vol. 3 (2 ed.). Detroit: Thomson/Gale. p. 137. ISBN 9780787663742.
12. "Computer and Internet Fraud". LII / Legal Information Institute. Archived from the original on 10 August 2022. Retrieved 1 November 2020.
13. Pratt, Travis C.; Holtfreter, Kristy; Reisig, Michael D. (2010). "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory". Journal of Research in Crime and Delinquency. 47 (3): 267–296. doi:10.1177/0022427810365903. S2CID 146182010.
14. What is ‘digital arrest’, and what can you do to ensure you don't fall victim to cybercriminals?, Indian Express, 17 May 2024.
15. Parker D (1983) Fighting Computer Crime, U.S.: Charles Scribner's Sons.
16. "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress". www.everycrsreport.com. Archived from the original on 29 September 2022. Retrieved 5 September 2021.
17. Morgan, Steve (13 November 2020). "Cybercrime To Cost The World $10.5 Trillion Annually By 2025". Cybercrime Magazine. Retrieved 19 July 2024.
18. Lepofsky, Ron. "Cyberextortion by Denial-of-Service Attack" (PDF). Archived from the original (PDF) on 6 July 2011.
19. Mohanta, Abhijit (6 December 2014). "Latest Sony Pictures Breach : A Deadly Cyber Extortion". Archived from the original on 25 September 2015. Retrieved 20 September 2015.
20. "Ransomware Trends 2024: Insights for Global Cybersecurity Readiness". www.cyberpeace.org. Retrieved 15 April 2025.