

# साइबर खतरे: अवधारणा, प्रकार और प्रवृत्तियाँ

# साइबर खतरे: अवधारणा

- आज के डिजिटल युग में इंटरनेट का उपयोग तेजी से बढ़ रहा है।
- ऑनलाइन बैंकिंग, सोशल मीडिया, ई-शिक्षा और ई-व्यापार के कारण साइबर सुरक्षा का महत्व बढ़ गया है।
- साइबर खतरे व्यक्तियों, संस्थाओं और देशों के लिए गंभीर चुनौती बन चुके हैं।

# साइबर खतरे: अवधारणा

- साइबर खतरा क्या है?
- ऐसी कोई भी गतिविधि जो कंप्यूटर, नेटवर्क, डेटा या डिजिटल प्रणाली को नुकसान पहुंचाए, साइबर खतरा कहलाती है।
- इसका उद्देश्य डेटा चोरी, गोपनीय जानकारी प्राप्त करना या सिस्टम को बाधित करना होता है।

# साइबर खतरे:

## साइबर खतरों की विशेषताएँ

- डिजिटल माध्यम से किए जाते हैं।
- तेजी से फैल सकते हैं।
- आर्थिक एवं सामाजिक नुकसान पहुँचाते हैं।
- व्यक्तिगत जानकारी को खतरे में डालते हैं।
- राष्ट्रीय सुरक्षा पर भी प्रभाव डाल सकते हैं।

# साइबर खतरे:

## साइबर खतरों के प्रमुख प्रकार

- वायरस (Virus)
- मालवेयर (Malware)
- फिशिंग (Phishing)
- रैनसमवेयर (Ransomware)
- हैकिंग (Hacking)
- स्पाइवेयर (Spyware)
- डिनायल ऑफ सर्विस अटैक (DoS Attack)

# वायरस (Virus)

- यह एक हानिकारक प्रोग्राम होता है।
- कंप्यूटर फाइलों को नुकसान पहुँचाता है।
- सिस्टम की गति धीमी कर देता है।
- एक कंप्यूटर से दूसरे कंप्यूटर में फैल सकता है।

# मालवेयर (Malware)

- “Malicious Software” का संक्षिप्त रूप।
- कंप्यूटर को नुकसान पहुँचाने के लिए बनाया जाता है।
- इसमें वायरस, ट्रोजन, वर्म आदि शामिल हैं।

# फिशिंग (Phishing)

- नकली ईमेल या वेबसाइट के माध्यम से जानकारी चुराना।
- पासवर्ड, बैंक विवरण और OTP चोरी किए जाते हैं।
- यह साइबर अपराध का सामान्य तरीका है।

# रैनसमवेयर (Ransomware)

- डेटा को लॉक कर देता है।
- डेटा वापस देने के बदले पैसे की मांग करता है।
- अस्पतालों, कंपनियों और सरकारी संस्थानों पर

# हैकिंग (Hacking)

- बिना अनुमति किसी सिस्टम में प्रवेश करना।
- डेटा चोरी या बदलाव करना।
- नैतिक (Ethical) और अनैतिक (Illegal) दोनों प्रकार की हो सकती है।

- **E-mail safety:** ई-मेल सुरक्षा
- **Safety in Social Networks:** सामाजिक नेटवर्क में सुरक्षा
- **Cyber Bullying & stalking:** साइबर बदमाशी और पीछा करना
- **Communication Ethics and soft skills while using email, chat, messenger or social networks;** ईमेल, चैट, मैसेंजर या सोशल नेटवर्क का उपयोग करते समय संचार नैतिकता और सॉफ्ट कौशल;
- **Password Safety:** पासवर्ड सुरक्षा:

# **E-mail safety:** ई-मेल सुरक्षा

- spam mail स्पैम मेल
- malicious links and how to avoid clicking them दुर्भावनापूर्ण लिंक और उन पर क्लिक करने से कैसे बचें, fraud emails with lucrative offers, etc.
- आकर्षक प्रस्तावों आदि के साथ धोखाधड़ी वाले ई-मेल।

# ई-मेल सुरक्षा

## **SCENARIO 1: -fraud emails with lucrative offers**

"Wow exclusive offer on gadgets offer valid for a limited period",

happy and clicked and downloaded the attached email to see more about the email after few minutes his system stopped working.

## **SCENARIO 2:-concept of spam mail**

Email with attachment from xyz@abcbank.com for updating the personal information to avoid blocking of his debit/credit card.

परिदृश्य 1:-आकर्षक प्रस्तावों के साथ धोखाधड़ी वाले ईमेल "वाह, गैजेट्स पर एक्सक्लूसिव ऑफर सीमित अवधि के लिए मान्य है", खुश होकर ईमेल के बारे में अधिक जानने के लिए संलग्न ईमेल को क्लिक किया और डाउनलोड किया, कुछ मिनटों के बाद उसके सिस्टम ने काम करना बंद कर दिया।

परिदृश्य 2:-स्पैम मेल अपने डेबिट/क्रेडिट कार्ड को ब्लॉक होने से बचाने के लिए

# ई-मेल सुरक्षा

## SCENARIO 3- SPOOFED EMAIL:

Consider Mr. Siddharth whose email address is `siddharth@hotmail.com`. His friend Ajay's email address is `ajay@yahoo.com`. Using FakeMail, Siddharth can send emails claiming to be sent from Ajay's email account. All he has to do is enter `ajay@yahoo.com` in the space provided for sender's email address. Ajay's friends would trust such emails, as they would suppose that they have come from Ajay whom they trust. Siddharth can use this misplaced trust to send viruses, Trojans, worms etc. to Ajay's friends, who would unknowingly download them.

## परिदृश्य 3- नकली ईमेल:

श्री सिद्धार्थ पर विचार करें जिनका ईमेल पता `siddharth@hotmail.com` है। उनके दोस्त अजय का ईमेल पता `ajay@yahoo.com` है। फेकमेल का उपयोग करके, सिद्धार्थ अजय के ईमेल खाते से भेजे जाने का दावा करते हुए ईमेल भेज सकता है। उसे बस प्रेषक के ईमेल पते के लिए दिए गए स्थान में `ajay@yahoo.com` दर्ज करना है। अजय के दोस्त ऐसे ईमेल पर भरोसा करेंगे, क्योंकि उन्हें लगेगा कि ये ईमेल अजय की ओर से आए हैं, जिस पर उन्हें भरोसा है। सिद्धार्थ इस गलत भरोसे का उपयोग अजय के दोस्तों को वायरस, ट्रोजन, कीड़े आदि भेजने के लिए कर सकता है जो अनजाने में

# Safety in Social Networks:

- **Identity protection,**
- **confidentiality and caution while dealing with anonymous or unknown;**
- पहचान की सुरक्षा,
- गुमनाम या अज्ञात के साथ व्यवहार करते समय गोपनीयता और सावधानी;

## साइबर खतरों से बचाव (How to Safeguard)

- मजबूत और अलग-अलग पासवर्ड का उपयोग करें।
- दो-स्तरीय सुरक्षा (Two-Factor Authentication) अपनाएँ।
- अज्ञात लिंक और ईमेल पर क्लिक न करें।
- सोशल मीडिया पर व्यक्तिगत जानकारी साझा करने से बचें।
- एंटीवायरस और फ़ायरवॉल का उपयोग करें।
- मोबाइल और कंप्यूटर को नियमित रूप से अपडेट करें।
- ऑनलाइन लेन-देन करते समय सुरक्षित वेबसाइट (HTTPS) का उपयोग करें।
- साइबर जागरूकता और डिजिटल सुरक्षा के नियमों का पालन करें।

# Password Safety:

- . पासवर्ड हमारी डिजिटल पहचान की सुरक्षा करता है।
- . मजबूत पासवर्ड हैकिंग और डेटा चोरी से बचाता है।
- . बैंकिंग, ईमेल और सोशल मीडिया खातों को सुरक्षित रखने के लिए आवश्यक है।
- . कमजोर पासवर्ड आसानी से अनुमान लगाए जा सकते हैं।
- . साइबर अपराधों से बचाव के लिए मजबूत पासवर्ड अत्यंत महत्वपूर्ण है।
- . पासवर्ड किसी के साथ साझा नहीं करना चाहिए।
- . पासवर्ड को कागज या मोबाइल नोट्स में खुला नहीं रखना चाहिए।
- . सार्वजनिक कंप्यूटर में "Remember Password" विकल्प का उपयोग न करें।
- . OTP और बैंकिंग पासवर्ड गोपनीय रखें।
- . साइबर ठग अक्सर नकली कॉल या ईमेल से पासवर्ड मांगते हैं।

# Don'ts

- ❖ ऐसे किसी ई-मेल या पॉप-अप संदेश का उत्तर न दें जो आपकी व्यक्तिगत या वित्तीय जानकारी माँगता हो।
- ❖ अपनी व्यक्तिगत या वित्तीय जानकारी, जैसे क्रेडिट कार्ड या अन्य संवेदनशील जानकारी, ई-मेल के माध्यम से साझा न करें।
- ❖ ऐसे किसी ई-मेल या सोशल मीडिया संदेश पर क्लिक न करें जिसकी आपको अपेक्षा न हो या जिसकी आवश्यकता न हो।
- ❖ ऐसे ई-मेल न खोलें जिन पर आपको संदेह हो कि वे वैध नहीं हैं। यदि वह वास्तव में वैध होगा और संपर्क करने वाले व्यक्ति को सच में आवश्यकता होगी, तो वह किसी अन्य माध्यम से संपर्क करेगा।
- ❖ ऐसे अटैचमेंट न खोलें जिनकी आपको अपेक्षा न हो, विशेष रूप से ZIP फाइलें, और कभी भी .exe फाइलें रन न करें।

# Don'ts

- अपनी कंपनी के ई-मेल पते का उपयोग व्यक्तिगत कार्यों के लिए न करें।
- किसी भी स्पैम ई-मेल को न खोलें।
- सोशल नेटवर्किंग साइट्स पर संदिग्ध वीडियो या चित्र न खोलें, क्योंकि सोशल नेटवर्किंग साइट्स फ़िशिंग का प्रमुख लक्ष्य होती हैं।
- बैंक विवरण माँगने वाले फोन कॉल्स का कभी उत्तर न दें। यह विंशिंग (वाँयस फ़िशिंग) हो सकता है।
- फ़िशिंग फोन कॉल्स से सावधान रहें।
- यदि आपको कोई संदेश (SMS) प्राप्त होता है जिसमें कहा जाए कि आपका खाता “चोरी” हो गया है या “खो” गया है और जानकारी की पुष्टि करने के लिए कहा जाए, या किसी पुरस्कार को प्राप्त करने के लिए व्यक्तिगत जानकारी साझा करने को कहा जाए, तो उसका उत्तर न दें। यह संभवतः फ़िशिंग का एक रूप है।

# misspelled URL



हमेशा किसी भी ऐसे ई-मेल अनुरोध को संदेह की दृष्टि से देखें जो वित्तीय या अन्य व्यक्तिगत जानकारी माँगता हो, विशेष रूप से वे अनुरोध जो “अत्यावश्यक” (urgent) बताए जाते हैं। यदि आपको संदेह हो, तो संदिग्ध ई-मेल का उत्तर न दें और न ही किसी संदिग्ध वेबसाइट पर अपनी जानकारी दर्ज करें। आप प्राप्त हुए संदेश की सत्यता की पुष्टि करने के लिए संबंधित प्रेषक (sender) से सीधे संपर्क भी कर सकते हैं।



ऐसे ई-मेल का कभी उत्तर न दें जो आपकी व्यक्तिगत जानकारी, जैसे क्रेडिट कार्ड, डेबिट कार्ड या बैंक संबंधी जानकारी माँगते हों।

**Income Tax Department**  
Department of Revenue, Ministry of Finance, Government of India

### Tax Refund

Get Tax Refund on your VISA or MasterCard

Please enter your EPF number and a valid Credit / Debit Card where you want the refund to be made.  
See our Privacy Notice regarding our request for your personal information.

EPF number #

**Credit / Debit Card**  
Please enter the following information here

Name on Card:

Issuing Bank:

Card Number:

Expiration Date:  /  (mm/yy)

CVV Code:

ATM Card PIN:  (PIN & its protection)

## **Communication Ethics and soft skills while using email, chat, messenger or social networks;**

### Illegal Content

sexually explicit, illegal images of sexual abuse, violence, criminal activity or accidents, from video clips, promotes extreme political views, potentially used in the radicalization of vulnerable members of the community

child abuse and unlawful hate speech. Age-inappropriate content on the sites, such as pornography or sexual content, violence

fake friends,

Online bullies

Hate speech:

Malicious links:

Always check the authenticity of the person before you accept a request

Don't give or post any personal information like your name, address of the school / home, phone numbers, age, sex, credit card details

Never post photographs, videos and any other sensitive information to unknown persons in Social network sites

Cyber Crime, IT Act, Cyber Law, Hacking, Fake websites, Phishing and other online frauds – caution and how to deal in such events; Copyright, Plagiarism and IPR issues; Software licensing -Proprietary software, Free and Open source software, Copyrighted vs Free resources, Creative Commons; E-waste, Radiation issue, Green Computing. ICT and potential of digital divide, mobile security, mobile app security(Health issue to be addressed)

साइबर अपराध, आईटी अधिनियम, साइबर कानून, हैकिंग, फर्जी वेबसाइट, फिशिंग और अन्य ऑनलाइन धोखाधड़ी - ऐसी घटनाओं से सावधानी और कैसे निपटें;

कॉपीराइट, साहित्यिक चोरी और आईपीआर मुद्दे; सॉफ्टवेयर लाइसेंसिंग - मालिकाना सॉफ्टवेयर, मुफ्त और मुक्त स्रोत सॉफ्टवेयर, कॉपीराइट बनाम मुफ्त समाधान, क्रिएटिव कॉमन्स; ई-कचरा, विकिरण मुद्दा, हरित कंप्यूटिंग। आईसीटी और डिजिटल विभाजन की संभावना, मोबाइल सुरक्षा, मोबाइल ऐप सुरक्षा (स्वास्थ्य मुद्दे का समाधान किया जाना है)

Threatening texts or unwanted e-mails  
Harassment  
Denigration  
Impersonating  
Outing: Sharing someone's secrets or embarrassing information or images online  
or  
Uploading victim's images by editing and uploading to a social networking sites  
Flaming: Online fights using vulgar messages or texts

## **IT Act Provisions Applicable:**

Sending threatening or extortive messages via e-mail/SMS/MMS. Sending of threat-mails and SMS is also punishable under section 506 (“punishment for criminal intimidation”) and section 507 (“criminal intimidation by an anonymous communication”) of the IPC.

Section 67 (“publishing or transmitting obscene material in electronic form”), IT Act.

Section 499 (“Defamation”) too can be used against the online abusers who try to harm the reputation through words.

Section 509 (“word, gesture or act intended to insult the modesty of a woman”) of the IPC

Creating a dedicated website with jokes, cartoons, gossip, and rumors about victim to damage his or her reputation.