Ministry of Electronics and Information Technology
Government of India

certin
Enhancing Cyber Security in India

CyberSmart

ᑲᕮᑭᘐᘓᗩᔑ

ᕮᕮᕱᕮᑭᗩᔑ ᘐᘓᗩ
ᑲᘐᗩᔑᘐᘓᗩᔑ ᑭᘐ.ᕱᗩᑭ
ᕮᘐᗩᔑᘐᘓᗩ ᑌᕮᕮᘐᕱ
ᗩᔑᑲᔑᗩᕮᕮᘐ. ᑲᘐᗩᔑᘐᘓᘐᑌᗩ



ᕮᔑᔑᘐ ᑭᘐ.ᕱᗩᑭ

National Cyber Security Awareness Month
(October 2026)

"Build a Culture of Cyber Hygiene"

#CyberHygieneOurCulture

ISEA Information Security Education & Awareness

Digital India Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

certin
Enhancing Cyber Security in India

ᔕᗩᖴᕮᔕᕼᗝᑭ

	ᑎᕮᑎᑭᑎᘜ	3
1	ᕮᘜᕮᔕᖴᕮᑭᑎᑭ ᔕᑫᑌᔕᖴᕮᔕᖴᕮᑭᘜᔕᔕ: "ᑭᑌᑭᘜ ᑭᘜ ᑌᑭᘜᘓᑭᑌᑭ?"	4
2	ᗪᘓᔕᕮᔕᔕ: "ᘜᑎᑌ ᑭᑭ.ᘜᔕᑭ ᑌᑭᘜᘓᑭᑌᑭ"	5
3	AI ᑌᑭ.ᗪᗝᔕ: "AI ᑭᑎᘓᑭ.ᗝ ᕮᑭᑌᑭ ᔕᑭᗪ ᑌᑕ?"	6
4	ᑌᑭᑭᑌᔕᖴᕮᑭᘜ: "ᕮᑭᑌᑭ ᕮᔕᑭᑌ ᘜᕮ ᑌᑭᘜᘓᑭᑌᑭ?"	7
5	ᘜᑎᑭᘓᔕᖴᕮᑭ. ᕮᕮᑎᕮᗪ ᘜᑎᑌ	8
	ᑭᑭᕮ ᕮᑭᑌ ᑌᘜᗪᑭᑌ ᑌᕮ	9



ᑲᕮᑲᑭᑲᑲᑫ

As students spend more time learning, communicating, collaborating, and creating online, understanding cybersecurity has become an essential life skill. Cyber threats are increasingly embedded in everyday digital experiences and may appear as a suspicious message, an unexpected login request, a misleading website, an unknown link, a deceptive voice or video, or a request for personal information. Equipping students with the knowledge to recognise these situations, pause, verify, and make informed decisions can help build safe and responsible digital habits from an early age.

The **Indian Computer Emergency Response Team (CERT-In's) CyberSmart Classroom: Scenario Based Cybersecurity Guide for Teachers & Students** provides teachers with practical and relatable scenarios that can be used to facilitate classroom discussions, activities, and interactive learning. Each scenario encourages students to identify potential risks, think critically, discuss possible responses, and understand simple cybersecurity best practices. By connecting cybersecurity concepts with situations students may encounter in their daily lives, the guide seeks to make cyber awareness engaging, relevant, and actionable, while fostering a culture of responsible digital citizenship.

This booklet has been published as part of **CERT-In National Cyber Security Awareness Month activities (October 2026)**, with the objective of strengthening cybersecurity awareness among students and educators. It is intended to support teachers in creating meaningful conversations around online safety and empowering students to make informed, secure, and responsible choices in the digital world.

1. ಕಂಪ್ಯೂಟರ್ ವ್ಯವಸ್ಥೆಗಳನ್ನು: "ನಮಗೆ ಅವು ಯಾವುವು?"



A **ಲಭ್ಯವಾಗಿರಬೇಕು**
ಯಾವುದೇ IT ವ್ಯವಸ್ಥೆಗೆ ಬೇಕಾದಾಗ।

U **ಅನಧಿಕೃತ**
ಯಾರಿಗೆ ಅನುಮತಿಸಲಾಗಿದೆಯೋ ಅವರು।

R **ಬದಲಾಯಿಸಲಾಗಿದೆ**
ಯಾವುದೇ ಅನಧಿಕೃತ।

F **ಪ್ರವೇಶ.ಬದಲಾವಣೆಯಾಗಿದೆ**
ಕಂಪ್ಯೂಟರ್ ಅಥವಾ ಡೇಟಾದ ಬೇಕಾದಾಗ।

ಸಲಹೆಗಳು

1. ಬಿಡುವಿಲ್ಲದ ಯಾವ ಬಿಡುವಿನ ಖಾತೆ.ಮೌಲ್ಯ ನೀಲಿಯ ಕೆಲಸದ IT ಸಂಸ್ಥೆಯ ಕೆಲಸಕ್ಕೆ ಬೇಕಾದ ಫೈಲ್‌ಗಳು ಬೇಕಾದಾಗ।

2. ಬಿಡುವಿಲ್ಲದ ಯಾವ ಡೇಟಾ ಬೇಕಾದ ಫೈಲ್‌ಗಳು ಬೇಡವಾದಾಗ।

3. ಬಿಡುವಿಲ್ಲದ ಯಾವ ಖಾತೆ.ಮೌಲ್ಯ ಬೇಕಾದ ಯಾರಿಗೆಯಾದರೂ ಬೇಡವಾದಾಗ।

4. ಬಿಡುವಿಲ್ಲದ ಯಾವ ಯಾವುದು ಬೇಡವಾದಾಗ।

ಖಾತೆ.ಲಾಗ್ ಯಾವುದು ಕೆಲಸಕ್ಕೆ ಯಾರಿಗೆ ಯಾವಾಗ

- ಲಭ್ಯವಾಗಿರಬೇಕು
- ಪ್ರವೇಶಿಸಲಾಗಿದೆ ಖಾತೆ.ಮೌಲ್ಯ ಯಾ
- ಯಾರಿಗೆಯಾದರೂ ಬೇಡವಾದಾಗ

ಯಾಕೆ ಕೆಲವರು:

Attackers may use urgency, authority, fear, curiosity, rewards, or familiarity to influence people.

1. ಫಿಶಿಂಗ್: "ನಮ್ಮ ಬ್ಯಾಂಕ್ ಅಕೌಂಟ್ ಅಮಾನತಾಗಿದೆ"

ಫಿಶಿಂಗ್ ಇಮೇಲ್‌ಗಳನ್ನು ಹೇಗೆ ಪತ್ತೆಹಚ್ಚುವುದು:

- ಅಪರಿಚಿತ ಕಳುಹಿಸುವವರಿಂದ ಬಂದಿರುವ ಇಮೇಲ್
- ಬ್ಯಾಂಕ್ ಅಥವಾ ಸರ್ಕಾರಿ ಸಂಸ್ಥೆಯಿಂದ ಬಂದಿರುವ ಇಮೇಲ್
- ಅನುಮಾನಾಸ್ಪದ ಲಗತ್ತುಗಳನ್ನು ಹೊಂದಿರುವ ಇಮೇಲ್
- ಫಿಶಿಂಗ್ ಇಮೇಲ್‌ಗಳಲ್ಲಿ ಸಾಮಾನ್ಯವಾಗಿ ಕಂಡುಬರುವ ಕಾಗುಣಿತ ಮತ್ತು ವ್ಯಾಕರಣ ದೋಷಗಳನ್ನು ಹೊಂದಿರುವ ಇಮೇಲ್
- ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳನ್ನು ಹೊಂದಿರುವ ಇಮೇಲ್
- ಫಿಶಿಂಗ್ ಇಮೇಲ್‌ಗಳಲ್ಲಿ ಸಾಮಾನ್ಯವಾಗಿ ಕಂಡುಬರುವ ಸಾಮಾನ್ಯ ಶುಭಾಶಯಗಳನ್ನು ಹೊಂದಿರುವ ಇಮೇಲ್
- ಅನುಮಾನಾಸ್ಪದ ಲಿಂಕ್‌ಗಳನ್ನು ಹೊಂದಿರುವ ಇಮೇಲ್ ಅನ್ನು ಗುರುತಿಸುವುದು ಹೇಗೆ

ಫಿಶಿಂಗ್

ಭದ್ರವಾಗಿರಿಸಿ

1. AI ሀ൩.ፐ0ፖ: "AI ൩ഗ൩൩.0 ൬൭ഗ൩ ധ൭൨ ሀፘ?"

ፐ൩൨ധ൩ഗ൨ഗധ ഗ൭ ዖ൩.ഭ൨ዋ ሄፘ൨ዋ ሀፘ:



ሀ൨൩ ፘ൨ഗ൨

AI can be useful, but students should protect personal information, verify important information, and consider the consequences of what they generate and share.

1. [illegible]



1. ఫిషింగ్ దాడులు ఎదుర్కోవడం ఎలా

ಹಾಡ ಲಹಾಯ

For reporting Cyber Security Incidents to CERT-In:

ಯಾಲಲ ಮಾಯಾಹಾಲ ಬಲ ಲಾಲಾಹಾಲ: https://www.cert-in.org.in/

ಯಾಮಾಹಾಲ: incident@cert-in.org.in

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

ಟಲಲ ಸಾಲಾಲ ಸಾಲಾಲಾಲಾಲ ಸಾಲಾಲಾಲ

ಟಲಲ: +91-11-22902657

ಲಲಟಲ ಸಾ ಟಲಾಲಾಲಾಲ ಸಾಲಾಲಾಲಾಲ ಬಾಲಾಲಾ ಸಾ ಲಲಾಲಾಲ ಪಾ.ಲಾಲಾ, ಯಾಮಾಹಾಲ ಬಲ ಲಾಲಾಲ:

training@cert-in.org.in

ಲಲಲಾಲ ಬಲ ಸಾಲಾಲಾಲ ಲಾ

@IndianCERT

@cert_india

ಟಲಲಾಲಾಲ ಬಲಾಲಾಲಾ

https://www.cert-in.org.in/AwarenessBooklets.jsp

ಸಬಬಾಲಾಲಾ. ಲಾಲಲಾಲಾ

https://www.csk.gov.in/security-tools.html

SCAN ME!