Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

ਸਾਈਬਰ ਸਮਾਰਟ ਕਲਾਸਰੂਮ

ਅਧਿਆਪਕਾਂ ਅਤੇ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਦ੍ਰਿਸ਼-ਆਧਾਰਿਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਮਾਰਗਦਰਸ਼ਿਕਾ



ਇਸ ਮੌਕੇ 'ਤੇ

ਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਮਹੀਨਾ

(ਅਕਤੂਬਰ 2026)

"ਸਾਈਬਰ ਹਾਈਜੀਨ ਦੀ ਸੰਸਕ੍ਰਿਤੀ ਬਣਾਓ"

#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

ਵਿਸ਼ਾ-ਸੂਚੀ

ਭੂਮਿਕਾ 3

1 ਸੋਸ਼ਲ ਇੰਜੀਨੀਅਰਿੰਗ: “ਭਰੋਸਾ ਜਾਂ ਧੋਖਾ?” 4

2 ਫਿਸ਼ਿੰਗ: “ਖ਼ਤਰੇ ਦੇ ਸੰਕੇਤ ਪਛਾਣੋ” 5

3 AI ਸੁਰੱਖਿਆ: “ਕੀ ਤੁਸੀਂ AI ਨੂੰ ਇਹ ਪੁੱਛੋਗੇ?” 6

4 ਮਾਲਵੇਅਰ: “ਇਹ ਅੰਦਰ ਕਿਵੇਂ ਆਉਂਦਾ ਹੈ?” 7

5 ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਏਸਕੇਪ ਰੂਮ 8

ਸਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰੋ 9



ਭੂਮਿਕਾ

ਜਿਵੇਂ ਵਿਦਿਆਰਥੀ ਆਨਲਾਈਨ ਸਿੱਖਣ, ਸੰਚਾਰ ਕਰਨ, ਸਹਿਯੋਗ ਕਰਨ ਅਤੇ ਰਚਨਾਤਮਕ ਕੰਮ ਕਰਨ ਵਿੱਚ ਵੱਧ ਸਮਾਂ ਬਿਤਾ ਰਹੇ ਹਨ, ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਨੂੰ ਸਮਝਣਾ ਜੀਵਨ ਦੀ ਇੱਕ ਜ਼ਰੂਰੀ ਕੌਸ਼ਲ ਬਣ ਗਿਆ ਹੈ। ਸਾਈਬਰ ਖ਼ਤਰੇ ਰੋਜ਼ਾਨਾ ਦੇ ਡਿਜ਼ਿਟਲ ਅਨੁਭਵਾਂ ਵਿੱਚ ਵੱਧ ਤੋਂ ਵੱਧ ਸ਼ਾਮਲ ਹੋ ਰਹੇ ਹਨ ਅਤੇ ਇਹ ਸ਼ੱਕੀ ਸੁਨੇਹੇ, ਅਚਾਨਕ ਲੌਗਇਨ ਬੇਨਤੀ, ਗੁੰਮਰਾਹ ਕਰਨ ਵਾਲੀ ਵੈੱਬਸਾਈਟ, ਅਣਜਾਣ ਲਿੰਕ, ਧੋਖੇਬਾਜ਼ ਆਵਾਜ਼ ਜਾਂ ਵੀਡੀਓ, ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਬੇਨਤੀ ਦੇ ਰੂਪ ਵਿੱਚ ਸਾਹਮਣੇ ਆ ਸਕਦੇ ਹਨ। ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਅਜਿਹੀਆਂ ਸਥਿਤੀਆਂ ਨੂੰ ਪਛਾਣਨ, ਰੁਕਣ, ਜਾਂਚ ਕਰਨ ਅਤੇ ਸੋਚ-ਸਮਝ ਕੇ ਫ਼ੈਸਲੇ ਲੈਣ ਦਾ ਗਿਆਨ ਦੇਣ ਨਾਲ ਛੋਟੀ ਉਮਰ ਤੋਂ ਹੀ ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਆਦਤਾਂ ਵਿਕਸਿਤ ਕਰਨ ਵਿੱਚ ਮਦਦ ਮਿਲ ਸਕਦੀ ਹੈ।

ਭਾਰਤੀ ਕੰਪਿਊਟਰ ਐਮਰਜੈਂਸੀ ਰਿਸਪਾਂਸ ਟੀਮ (CERT-In) ਦੀ 'ਸਾਈਬਰ ਸਮਾਰਟ ਕਲਾਸਰੂਮ: ਅਧਿਆਪਕਾਂ ਅਤੇ ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਦ੍ਰਿਸ਼-ਆਧਾਰਿਤ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਮਾਰਗਦਰਸ਼ਿਕਾ' ਅਧਿਆਪਕਾਂ ਨੂੰ ਵਿਹਾਰਕ ਅਤੇ ਜਾਣ-ਪਛਾਣ ਵਾਲੇ ਦ੍ਰਿਸ਼ ਪ੍ਰਦਾਨ ਕਰਦੀ ਹੈ, ਜਿਨ੍ਹਾਂ ਦੀ ਵਰਤੋਂ ਕਲਾਸਰੂਮ ਚਰਚਾਵਾਂ, ਗਤੀਵਿਧੀਆਂ ਅਤੇ ਇੰਟਰਐਕਟਿਵ ਸਿੱਖਣ ਨੂੰ ਸੁਗਮ ਬਣਾਉਣ ਲਈ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ। ਹਰ ਦ੍ਰਿਸ਼ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਸੰਭਾਵਿਤ ਖ਼ਤਰਿਆਂ ਦੀ ਪਛਾਣ ਕਰਨ, ਆਲੋਚਨਾਤਮਕ ਢੰਗ ਨਾਲ ਸੋਚਣ, ਸੰਭਾਵਿਤ ਪ੍ਰਤੀਕਿਰਿਆਵਾਂ ਬਾਰੇ ਚਰਚਾ ਕਰਨ ਅਤੇ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੀਆਂ ਸਧਾਰਣ ਸਰਵੋਤਮ ਪ੍ਰਥਾਵਾਂ ਨੂੰ ਸਮਝਣ ਲਈ ਉਤਸ਼ਾਹਿਤ ਕਰਦਾ ਹੈ। ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਦੇ ਸੰਕਲਪਾਂ ਨੂੰ ਉਹਨਾਂ ਸਥਿਤੀਆਂ ਨਾਲ ਜੋੜ ਕੇ, ਜਿਨ੍ਹਾਂ ਦਾ ਵਿਦਿਆਰਥੀ ਆਪਣੀ ਰੋਜ਼ਾਨਾ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਸਾਹਮਣਾ ਕਰ ਸਕਦੇ ਹਨ, ਇਹ ਮਾਰਗਦਰਸ਼ਿਕਾ ਸਾਈਬਰ ਜਾਗਰੂਕਤਾ ਨੂੰ ਰੁਚਿਕਰ, ਪ੍ਰਸੰਗਿਕ ਅਤੇ ਅਮਲਯੋਗ ਬਣਾਉਣ ਦੇ ਨਾਲ-ਨਾਲ ਜ਼ਿੰਮੇਵਾਰ ਡਿਜ਼ਿਟਲ ਨਾਗਰਿਕਤਾ ਦੀ ਸੰਸਕ੍ਰਿਤੀ ਨੂੰ ਉਤਸ਼ਾਹਿਤ ਕਰਨ ਦਾ ਉਦੇਸ਼ ਰੱਖਦੀ ਹੈ।

ਇਹ ਪੁਸਤਿਕਾ CERT-In ਦੇ ਰਾਸ਼ਟਰੀ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਮਹੀਨਾ ਗਤੀਵਿਧੀਆਂ (ਅਕਤੂਬਰ 2026) ਦੇ ਹਿੱਸੇ ਵਜੋਂ ਪ੍ਰਕਾਸ਼ਿਤ ਕੀਤੀ ਗਈ ਹੈ, ਜਿਸ ਦਾ ਉਦੇਸ਼ ਵਿਦਿਆਰਥੀਆਂ ਅਤੇ ਸਿੱਖਿਆਕਾਰਾਂ ਵਿੱਚ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਜਾਗਰੂਕਤਾ ਨੂੰ ਮਜ਼ਬੂਤ ਕਰਨਾ ਹੈ। ਇਸ ਦਾ ਉਦੇਸ਼ ਅਧਿਆਪਕਾਂ ਨੂੰ ਆਨਲਾਈਨ ਸੁਰੱਖਿਆ ਬਾਰੇ ਅਰਥਪੂਰਨ ਗੱਲਬਾਤ ਕਰਨ ਅਤੇ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਡਿਜ਼ਿਟਲ ਸੰਸਾਰ ਵਿੱਚ ਸੋਚ-ਸਮਝ ਕੇ, ਸੁਰੱਖਿਅਤ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰ ਚੋਣਾਂ ਕਰਨ ਲਈ ਸਸ਼ਕਤ ਬਣਾਉਣ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਨਾ ਹੈ।

1. ਸੋਸ਼ਲ ਇੰਜੀਨੀਅਰਿੰਗ: “ਭਰੋਸਾ ਜਾਂ ਧੋਖਾ?”



A **ਅਧਿਕਾਰ**
ਮੈਂ IT ਵਿਭਾਗ ਤੋਂ ਹਾਂ।

U **ਤੁਰੰਤਤਾ**
ਤੁਰੰਤ ਕਾਰਵਾਈ ਕਰੋ।

R **ਇਨਾਮ**
ਮੁਫ਼ਤ ਡਾਊਨਲੋਡ।

F **ਜਾਣ-ਪਛਾਣ**
ਇਹ ਤੁਹਾਡਾ ਦੋਸਤ ਹੈ।

ਸੰਕੇਤ

1. ਕੋਈ ਵਿਅਕਤੀ ਸਕੂਲ ਦੇ IT ਵਿਭਾਗ ਤੋਂ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਕੇ ਫ਼ੋਨ ਕਰਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਮੰਗਦਾ ਹੈ।
2. ਕੋਈ ਵਿਅਕਤੀ ਕਹਿੰਦਾ ਹੈ ਕਿ ਉਹ ਤੁਹਾਡਾ ਦੋਸਤ ਹੈ, ਪਰ ਨਵਾਂ ਖਾਤਾ ਵਰਤ ਰਿਹਾ ਹੈ ਅਤੇ ਤੁਰੰਤ ਪੈਸੇ ਟ੍ਰਾਂਸਫ਼ਰ ਕਰਨ ਲਈ ਕਹਿੰਦਾ ਹੈ।
3. ਕੋਈ ਵਿਅਕਤੀ ਤੁਹਾਡੇ ਲੌਗਇਨ ਵੇਰਵਿਆਂ ਦੇ ਬਦਲੇ ਮੁਫ਼ਤ ਗੇਮ ਡਾਊਨਲੋਡ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦਾ ਹੈ।
4. ਇੱਕ ਵਿਦਿਆਰਥੀ ਨੂੰ ਸੁਨੇਹਾ ਮਿਲਦਾ ਹੈ ਕਿ ਜੇਕਰ ਉਹ ਤੁਰੰਤ ਕਾਰਵਾਈ ਨਾ ਕਰੇ ਤਾਂ ਉਸਦਾ ਖਾਤਾ ਮਿਟਾ ਦਿੱਤਾ ਜਾਵੇਗਾ।

ਫ਼ੈਸਲੇ ਦਾ ਰਸਤਾ

🟢 ਸੰਭਵਤੌਰ 'ਤੇ ਸੁਰੱਖਿਅਤ | 🟡 ਪੁਸ਼ਟੀ ਦੀ ਲੋੜ ਹੈ | 🔴 ਸੰਭਾਵਿਤ ਹੇਰਾਫੇਰੀ

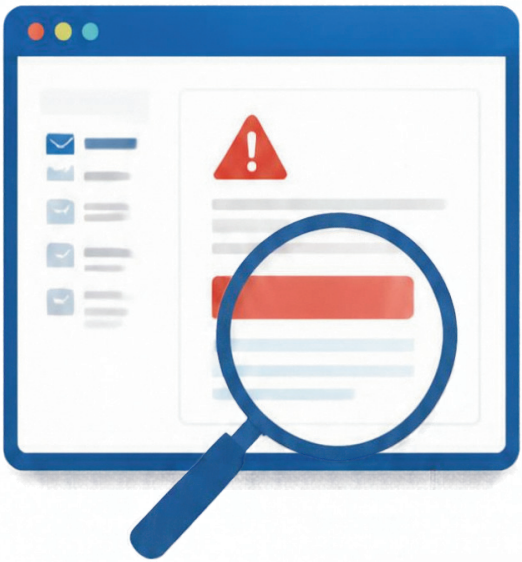
ਮੁੱਖ ਸਿੱਖਿਆ:

ਹਮਲਾਵਰ ਲੋਕਾਂ ਨੂੰ ਪ੍ਰਭਾਵਿਤ ਕਰਨ ਲਈ ਤੁਰੰਤਤਾ, ਅਧਿਕਾਰ, ਡਰ, ਜਿਗਿਆਸਾ, ਇਨਾਮ ਜਾਂ ਜਾਣ-ਪਛਾਣ ਦਾ ਸਹਾਰਾ ਲੈ ਸਕਦੇ ਹਨ।

2. ਫਿਸ਼ਿੰਗ: “ਖ਼ਤਰੇ ਦੇ ਸੰਕੇਤ ਪਛਾਣੋ”

ਵਿਦਿਆਰਥੀਆਂ ਲਈ ਯਾਦ ਰੱਖਣ ਵਾਲਾ ਨਿਯਮ:

ਰੁਕੋ → ਜਾਂਚੋ → ਪੁਸ਼ਟੀ ਕਰੋ → ਰਿਪੋਰਟ ਕਰੋ





ਸੁਰੱਖਿਅਤ



ਫਿਸ਼ਿੰਗ

- ਸ਼ੱਕੀ ਭੇਜਣ ਵਾਲੇ ਦੇ ਪਤੇ
- ਤੁਰੰਤਤਾ ਜਾਂ ਧਮਕੀ ਭਰੀ ਭਾਸ਼ਾ
- ਅਣਉਮੀਦ ਅਟੈਚਮੈਂਟ
- ਪਾਸਵਰਡ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਲਈ ਬੇਨਤੀਆਂ
- ਸ਼ੱਕੀ ਲਿੰਕ
- ਸ਼ਬਦ-ਜੋੜ ਜਾਂ ਵਿਆਕਰਨ ਦੀਆਂ ਗ਼ਲਤੀਆਂ
- ਅਸਧਾਰਣ ਭੁਗਤਾਨ ਦੀਆਂ ਬੇਨਤੀਆਂ
- ਮੇਲ ਨਾ ਖਾਂਦੇ ਵੈੱਬਸਾਈਟ ਪਤੇ

3. AI ਸੁਰੱਖਿਆ: “ਕੀ ਤੁਸੀਂ AI ਨੂੰ ਇਹ ਪੁੱਛੋਗੇ?”

ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਇਨ੍ਹਾਂ ਬਾਰੇ ਸਿਖਾਓ:

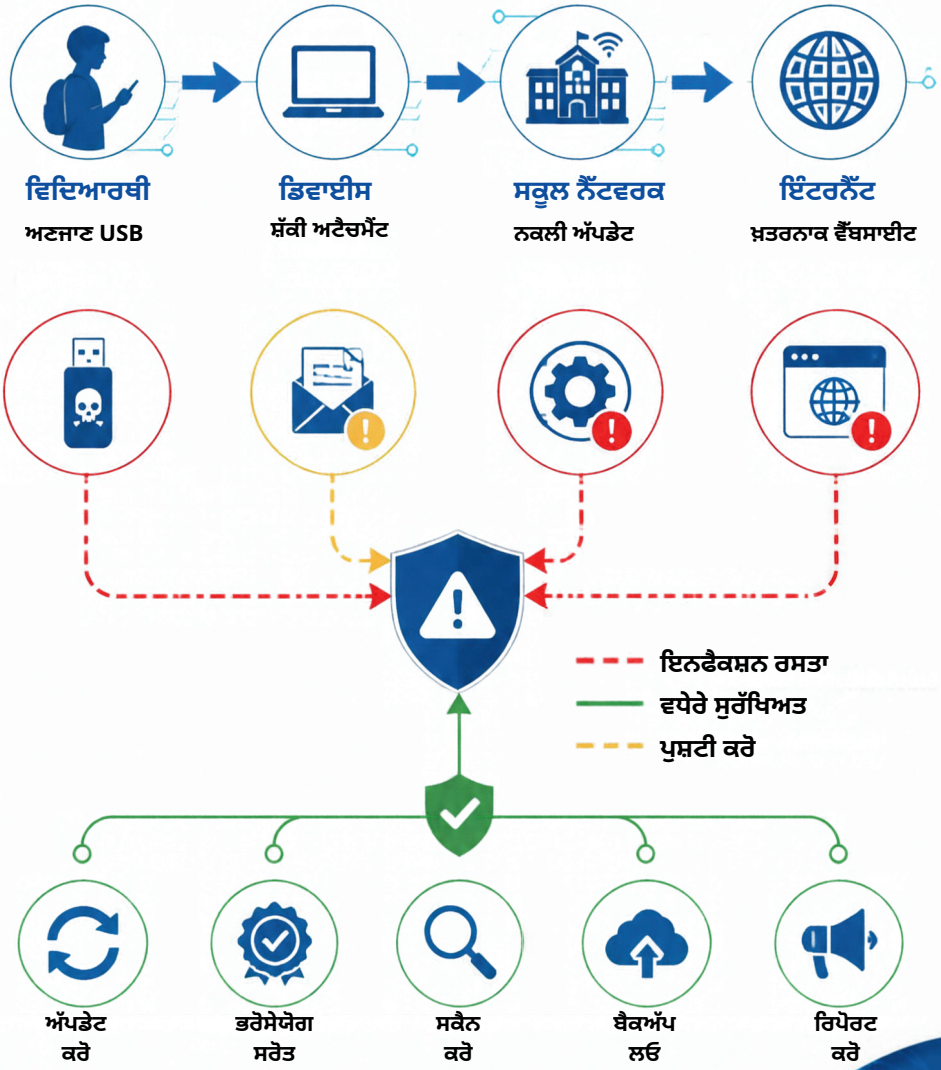


1. ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਕਰੋ
2. ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ
3. ਨਤੀਜਿਆਂ ਬਾਰੇ ਸੋਚੋ
4. ਜ਼ਿੰਮੇਵਾਰ ਵਰਤੋਂ

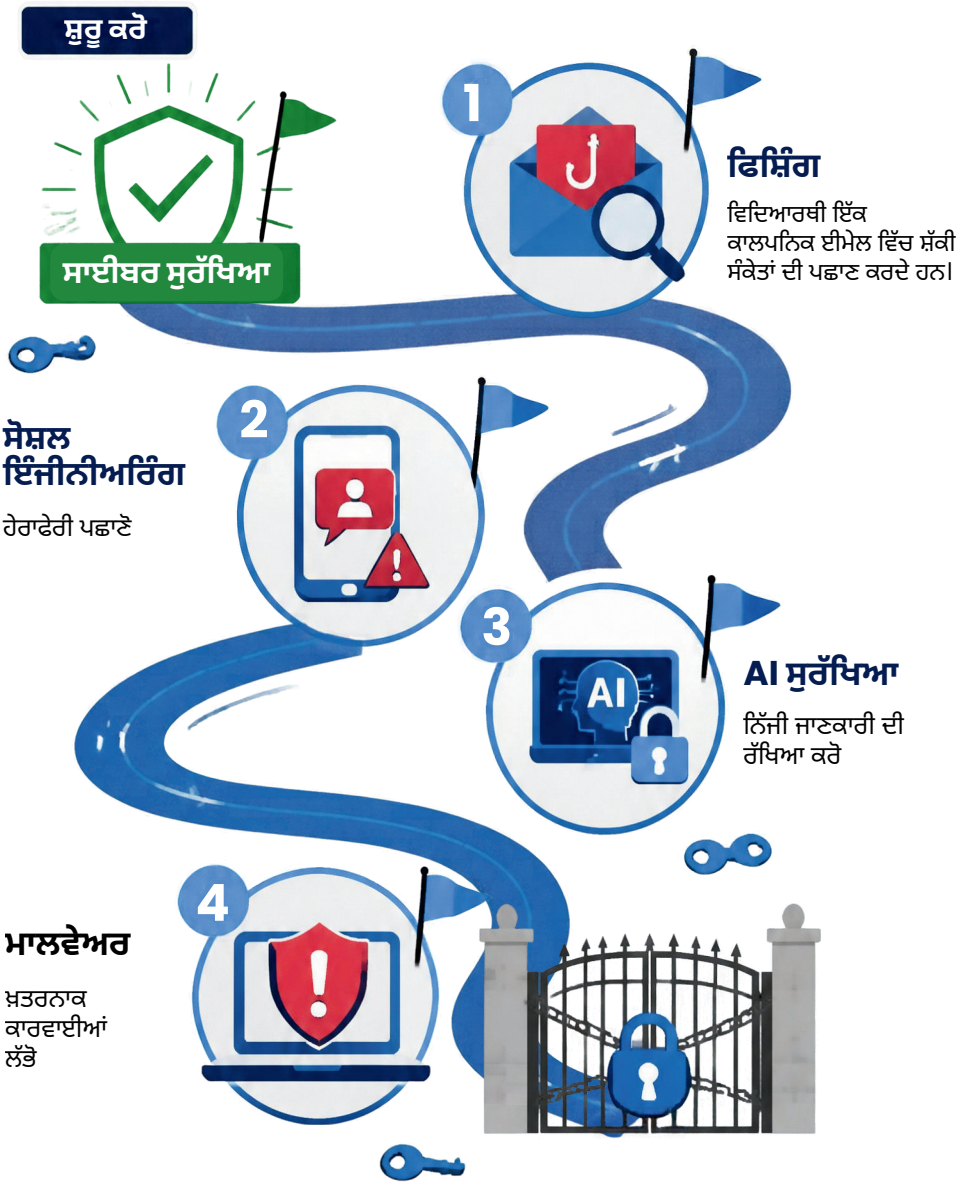
ਮੁੱਖ ਸਿੱਖਿਆ

AI ਲਾਭਦਾਇਕ ਹੋ ਸਕਦਾ ਹੈ, ਪਰ ਵਿਦਿਆਰਥੀਆਂ ਨੂੰ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ, ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨੀ ਚਾਹੀਦੀ ਹੈ ਅਤੇ ਜੋ ਕੁਝ ਉਹ ਬਣਾਉਂਦੇ ਅਤੇ ਸਾਂਝਾ ਕਰਦੇ ਹਨ, ਉਸ ਦੇ ਨਤੀਜਿਆਂ ਬਾਰੇ ਸੋਚਣਾ ਚਾਹੀਦਾ ਹੈ।

4. ਮਾਲਵੇਅਰ: “ਇਹ ਅੰਦਰ ਕਿਵੇਂ ਆਉਂਦਾ ਹੈ?”



5. ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਏਸਕੇਪ ਰੂਮ



ਸਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰੋ

CERT-In ਨੂੰ ਸਾਈਬਰ ਸੁਰੱਖਿਆ ਘਟਨਾਵਾਂ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਲਈ:

- **ਵੈੱਬਸਾਈਟ ਵੇਖੋ:** https://www.cert-in.org.in/
- **ਈਮੇਲ:** incident@cert-in.org.in
- **ਟੋਲ-ਫ੍ਰੀ ਫ਼ੋਨ:** +91-1800-11-4949
- **ਟੋਲ-ਫ੍ਰੀ ਫੈਕਸ:** +91-1800-11-6969

ਜਾਣਕਾਰੀ ਡੈਸਕ

- **ਫ਼ੋਨ:** +91-11-22902657

ਟ੍ਰੇਨਿੰਗ ਅਤੇ ਜਾਗਰੂਕਤਾ ਸੈਸ਼ਨਾਂ ਵਿੱਚ ਭਾਗ ਲੈਣ ਲਈ, ਈਮੇਲ ਕਰੋ:
training@cert-in.org.in

ਸਾਨੂੰ ਇੱਥੇ ਫਾਲੋ ਕਰੋ

@IndianCERT

@cert_india

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

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

SCAN ME!