Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

ସାଇବର ସଚେତନ ଗ୍ରେଣୀକକ୍ଷ

ପରିସ୍ଥିତି ଆଧାରିତ ସାଇବର ସୁରକ୍ଷା ମାର୍ଗଦର୍ଶିକା: ଶିକ୍ଷକ ଓ ଛାତ୍ରଛାତ୍ରୀଙ୍କ ପାଇଁ



ଅବସରରେ

ଜାତୀୟ ସାଇବର ସୁରକ୍ଷା ସଚେତନତା ମାସ
(ଅକ୍ଟୋବର ୨୦୨୬)

“ସାଇବର ସ୍ୱଚ୍ଛତାର ସଂସ୍କୃତି ଗଢ଼ି ତୋଳନ୍ତୁ”

#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

ବିଷୟସୂଚୀ

	ପ୍ରାକ୍କଥନ	3
1	ସୋସିଆଲ୍ ଇଞ୍ଜିନିୟରିଂ: “ବିଶ୍ୱାସ ନା ପ୍ରତାରଣା?”	4
2	ଫିଶିଂ: “ସତର୍କ ସଙ୍କେତଗୁଡ଼ିକ ଚିହ୍ନଟ କରନ୍ତୁ”	5
3	AI ସୁରକ୍ଷା: “ଆପଣ AIକୁ ଏହା ପଚାରିବେ କି?”	6
4	ମାଲୱେର୍: “ଏହା କିପରି ପ୍ରବେଶ କରେ?”	7
5	ସାଇବର ସୁରକ୍ଷା ଏସ୍କେପ୍ ରୁମ୍	8
	ଆମ ସହିତ ଯୋଗାଯୋଗ କରନ୍ତୁ	9



ପ୍ରାକ୍କଥନ

ଛାତ୍ରଛାତ୍ରୀମାନେ ଅନଲାଇନ୍‌ରେ ଶିକ୍ଷା ଗ୍ରହଣ, ଯୋଗାଯୋଗ, ସହଯୋଗ ଏବଂ ସୃଜନଶୀଳ କାର୍ଯ୍ୟରେ ଅଧିକ ସମୟ ବିତାଉଥିବାରୁ, ସାଇବର ସୁରକ୍ଷା ବୁଝିବା ଏକ ଆବଶ୍ୟକ ଜୀବନଦକ୍ଷତା ହୋଇପଡ଼ିଛି। ସାଇବର ଆକ୍ରମଣର ଆଶଙ୍କା ଦୈନନ୍ଦିନ ଡିଜିଟାଲ୍ ଅନୁଭବରେ କ୍ରମେ ଅଧିକ ଜଡ଼ିତ ହେଉଛି ଏବଂ ଏହା ସନ୍ଦେହଜନକ ବାର୍ତ୍ତା, ଅପେକ୍ଷାତୀତ ଲଗଇନ୍ ଅନୁରୋଧ, ଭ୍ରମଜନକ ୱେବସାଇଟ୍, ଅଜଣା ଲିଙ୍କ୍, ଠକେଇପୂର୍ଣ୍ଣ ଧ୍ୱନି କିମ୍ବା ଭିଡିଓ, କିମ୍ବା ବ୍ୟକ୍ତିଗତ ସୂଚନା ଚାହୁଁଥିବା ଅନୁରୋଧ ରୂପେ ଦେଖାଦେଇପାରେ। ଏପରି ପରିସ୍ଥିତିକୁ ଚିହ୍ନଟ କରିବା, ଥମ୍ଭିବା, ଯାଞ୍ଚ କରିବା ଏବଂ ସୂଚନାଭିତ୍ତିକ ନିଷ୍ପତ୍ତି ନେବା ପାଇଁ ଛାତ୍ରଛାତ୍ରୀମାନଙ୍କୁ ଜ୍ଞାନ ଦେବା ଦ୍ୱାରା ଅଳ୍ପ ବୟସରୁ ସୁରକ୍ଷିତ ଓ ଦାୟିତ୍ୱଶୀଳ ଡିଜିଟାଲ୍ ଅଭ୍ୟାସ ଗଢ଼ି ତୋଳିବାରେ ସାହାଯ୍ୟ ମିଳିପାରେ।

ଭାରତୀୟ କମ୍ପ୍ୟୁଟର ଆପାତକାଳୀନ ପ୍ରତିକ୍ରିୟା ଦଳ (CERT-In)ର 'ସାଇବରସ୍ମାର୍ଟ କ୍ଲାସରୁମ୍: ଶିକ୍ଷକ ଓ ଛାତ୍ରଛାତ୍ରୀଙ୍କ ପାଇଁ ପରିସ୍ଥିତି ଆଧାରିତ ସାଇବର ସୁରକ୍ଷା ମାର୍ଗଦର୍ଶିକା' ଶିକ୍ଷକମାନଙ୍କୁ ଏପରି ବ୍ୟବହାରିକ ଏବଂ ସହଜରେ ସମ୍ପର୍କିତ ପରିସ୍ଥିତି ପ୍ରଦାନ କରେ, ଯାହାକୁ ଶ୍ରେଣୀକକ୍ଷ ଆଲୋଚନା, କାର୍ଯ୍ୟକଳାପ ଏବଂ ପାରସ୍ପରିକ ଶିକ୍ଷଣରେ ବ୍ୟବହାର କରାଯାଇପାରେ। ପ୍ରତ୍ୟେକ ପରିସ୍ଥିତି ଛାତ୍ରଛାତ୍ରୀମାନଙ୍କୁ ସମ୍ଭାବ୍ୟ ବିପଦ ଚିହ୍ନଟ କରିବା, ସମାଲୋଚନାତ୍ମକ ଭାବେ ଚିନ୍ତା କରିବା, ସମ୍ଭାବ୍ୟ ପ୍ରତିକ୍ରିୟା ଉପରେ ଆଲୋଚନା କରିବା ଏବଂ ସରଳ ସାଇବର ସୁରକ୍ଷାର ଉତ୍ତମ ପଦ୍ଧତି ବୁଝିବାକୁ ପ୍ରୋତ୍ସାହିତ କରେ। ଛାତ୍ରଛାତ୍ରୀମାନେ ଦୈନନ୍ଦିନ ଜୀବନରେ ସାମ୍ନା କରିପାରୁଥିବା ପରିସ୍ଥିତି ସହିତ ସାଇବର ସୁରକ୍ଷାର ଧାରଣାଗୁଡ଼ିକୁ ଯୋଡ଼ି, ଏହି ମାର୍ଗଦର୍ଶିକା ସାଇବର ସଚେତନତାକୁ ଆକର୍ଷଣୀୟ, ପ୍ରାସଙ୍ଗିକ ଏବଂ ପ୍ରୟୋଗଯୋଗ୍ୟ କରିବା ସହିତ ଦାୟିତ୍ୱଶୀଳ ଡିଜିଟାଲ୍ ନାଗରିକତାର ସଂସ୍କୃତି ଗଢ଼ି ତୋଳିବାକୁ ଲକ୍ଷ୍ୟ ରଖେ।

ଏହି ପୁସ୍ତିକାଟି CERT-Inର ଜାତୀୟ ସାଇବର ସୁରକ୍ଷା ସଚେତନତା ମାସ (ଅକ୍ଟୋବର ୨୦୨୬) କାର୍ଯ୍ୟକ୍ରମର ଅଂଶ ଭାବେ ପ୍ରକାଶିତ ହୋଇଛି। ଛାତ୍ରଛାତ୍ରୀ ଓ ଶିକ୍ଷକମାନଙ୍କ ମଧ୍ୟରେ ସାଇବର ସୁରକ୍ଷା ସଚେତନତାକୁ ସୁଦୃଢ଼ କରିବା ଏହାର ଉଦ୍ଦେଶ୍ୟ। ଅନଲାଇନ୍ ସୁରକ୍ଷା ବିଷୟରେ ଅର୍ଥପୂର୍ଣ୍ଣ ଆଲୋଚନା ସୃଷ୍ଟି କରିବାରେ ଶିକ୍ଷକମାନଙ୍କୁ ସହାୟତା କରିବା ଏବଂ ଡିଜିଟାଲ୍ ଜଗତରେ ସୂଚନାଭିତ୍ତିକ, ସୁରକ୍ଷିତ ଓ ଦାୟିତ୍ୱଶୀଳ ନିଷ୍ପତ୍ତି ନେବା ପାଇଁ ଛାତ୍ରଛାତ୍ରୀମାନଙ୍କୁ ସକ୍ଷମ କରିବା ଏହାର ଲକ୍ଷ୍ୟ।

1. ସୋସିଆଲ୍ ଇଞ୍ଜିନିୟରିଂ: "ବିଶ୍ୱାସ ନା ପ୍ରତାରଣା?"



A **କର୍ତ୍ତୃତ୍ୱ**
ମୁଁ IT ବିଭାଗରୁ କହୁଛି।

U **ତତ୍ପରତା**
ତୁରନ୍ତ କାର୍ଯ୍ୟ କରନ୍ତୁ।

R **ପୁରସ୍କାର**
ମାଗଣା ଡାଉନଲୋଡ୍।

F **ପରିଚିତତା**
ଏହା ଆପଣଙ୍କ ବନ୍ଧୁ।

ସଙ୍କେତଗୁଡ଼ିକ

1. ଜଣେ ବ୍ୟକ୍ତି ସ୍କୁଲ୍‌ର IT ବିଭାଗରୁ ବୋଲି ଦାବି କରି ଫୋନ୍ କରନ୍ତି ଏବଂ ଆପଣଙ୍କ ପାସୱାର୍ଡ ମାଗନ୍ତି।

2. ଜଣେ ବ୍ୟକ୍ତି ନିଜକୁ ଆପଣଙ୍କ ବନ୍ଧୁ ବୋଲି କହୁଛନ୍ତି, କିନ୍ତୁ ଏକ ନୂଆ ଆକାଉଣ୍ଟ ବ୍ୟବହାର କରି ତୁରନ୍ତ ଟଙ୍କା ପଠାଇବାକୁ କହୁଛନ୍ତି।

3. ଜଣେ ବ୍ୟକ୍ତି ଆପଣଙ୍କ ଲଗଇନ୍ ବିବରଣୀ ବଦଳରେ ମାଗଣା ଗେମ୍ ଡାଉନଲୋଡ୍ ଦେବାକୁ ପ୍ରସ୍ତାବ ଦେଉଛନ୍ତି।

4. ଜଣେ ଛାତ୍ର କିମ୍ବା ଛାତ୍ରୀଙ୍କୁ ଏକ ବାର୍ତ୍ତା ମିଳେ ଯେ, ସେ ତୁରନ୍ତ କାର୍ଯ୍ୟ ନ କଲେ ତାଙ୍କ ଆକାଉଣ୍ଟ ବିଲୋପ କରାଯିବ।

ନିଷ୍ପତ୍ତି ପଥ

🟢 ସମ୍ଭବତଃ ସୁରକ୍ଷିତ | 🟡 ଯାଞ୍ଚ ଆବଶ୍ୟକ | 🔴 ସମ୍ଭାବ୍ୟ ପ୍ରତାରଣା

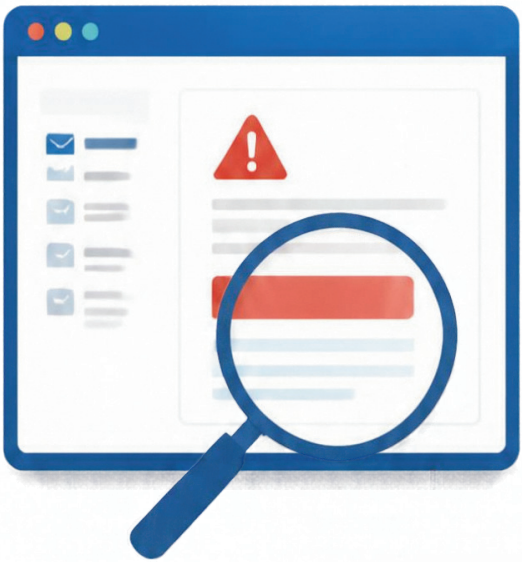
ମୁଖ୍ୟ ଶିକ୍ଷା:

ଆକ୍ରମଣକାରୀମାନେ ଲୋକମାନଙ୍କୁ ପ୍ରଭାବିତ କରିବା ପାଇଁ ତତ୍ପରତା, କର୍ତ୍ତୃତ୍ୱ, ଭୟ, କୌତୁହଳ, ପୁରସ୍କାର କିମ୍ବା ପରିଚିତତାର ବ୍ୟବହାର କରିପାରନ୍ତି।

2. ଫିଶିଂ: "ସତର୍କ ସଙ୍କେତଗୁଡ଼ିକ ଚିହ୍ନଟ କରନ୍ତୁ"

ଛାତ୍ରଛାତ୍ରୀମାନେ ମନେ ରଖିବା ଉଚିତ ନିୟମ:







SAFE



PHISHING

- ସନ୍ଦେହଜନକ ପ୍ରେଷକଙ୍କ ଠିକଣା
- ତତ୍ପାଳିକ କିମ୍ବା ଧମକପୂର୍ଣ୍ଣ ଭାଷା
- ଅପେକ୍ଷାତୀତ ସଂଲଗ୍ନ ଫାଇଲ୍
- ପାସୱାର୍ଡ କିମ୍ବା ବ୍ୟକ୍ତିଗତ ସୂଚନା ପାଇଁ ଅନୁରୋଧ
- ସନ୍ଦେହଜନକ ଲିଙ୍କ୍
- ବନାନ/ବ୍ୟାକରଣର ଅସଙ୍ଗତି
- ଅସାଧାରଣ ଦେୟ ଅନୁରୋଧ
- ମେଳ ନଥିବା ୱେବସାଇଟ୍ ଠିକଣା

3. AI ସୁରକ୍ଷା: “ଆପଣ AIକୁ ଏହା ପଚାରିବେ କି?”

ଛାତ୍ରଛାତ୍ରୀମାନଙ୍କୁ ଏହି ବିଷୟରେ ଶିଖାନ୍ତୁ:

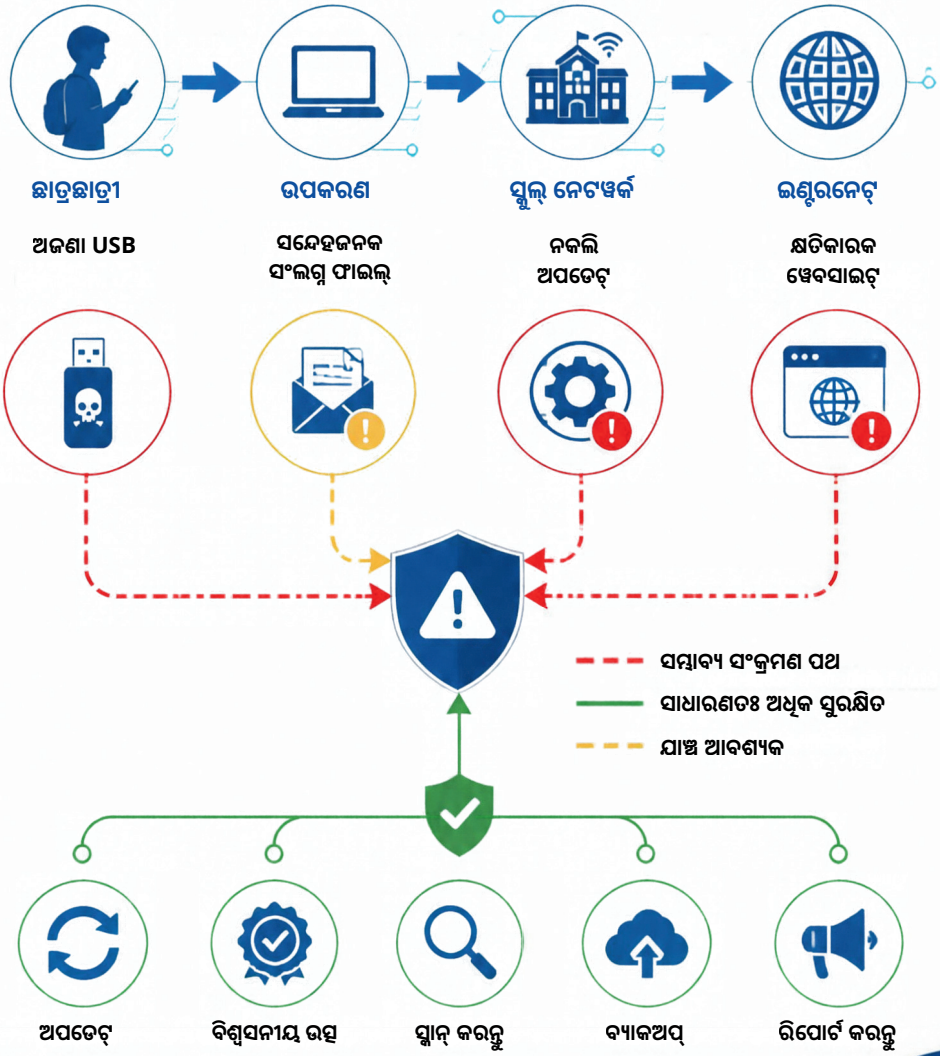


1. ବ୍ୟକ୍ତିଗତ ସୂଚନା ସୁରକ୍ଷିତ ରଖନ୍ତୁ
2. ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ସୂଚନା ଯାଞ୍ଚ କରନ୍ତୁ
3. ପରିଣାମ ବିଷୟରେ ବିଚାର କରନ୍ତୁ
4. ଦାୟିତ୍ୱଶୀଳ ବ୍ୟବହାର

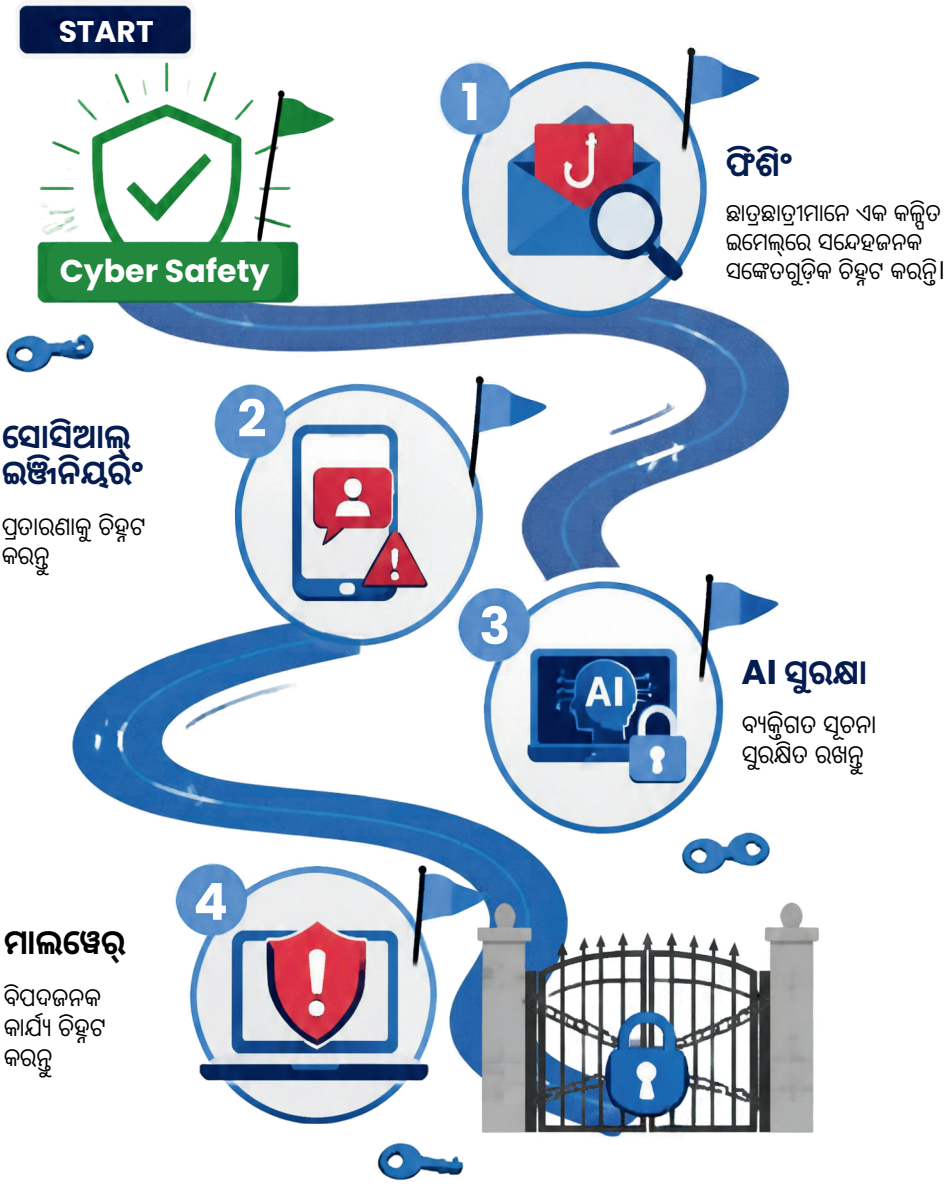
ମୁଖ୍ୟ ଶିକ୍ଷା

AI ଉପଯୋଗୀ ହୋଇପାରେ, କିନ୍ତୁ ଛାତ୍ରଛାତ୍ରୀମାନେ ବ୍ୟକ୍ତିଗତ ସୂଚନା ସୁରକ୍ଷିତ ରଖିବା, ଗୁରୁତ୍ୱପୂର୍ଣ୍ଣ ସୂଚନା ଯାଞ୍ଚ କରିବା ଏବଂ ସେମାନେ ସୃଷ୍ଟି କରି ସେୟାର୍ କରୁଥିବା ବିଷୟର ପରିଣାମ ବିଷୟରେ ବିଚାର କରିବା ଉଚିତ।

4. ମାଲୱେର୍: “ଏହା କିପରି ପ୍ରବେଶ କରେ?”



5. ସାଇବର ସୁରକ୍ଷା ଏସ୍କେପ୍ ରୁମ୍



ଆମ ସହିତ

CERT-Inକୁ ସାଇବର ସୁରକ୍ଷା ଘଟଣା ରିପୋର୍ଟ କରିବା ପାଇଁ:

- **ୱେବସାଇଟ୍ ଦେଖନ୍ତୁ:** https://www.cert-in.org.in/
- **ଇମେଲ୍:** incident@cert-in.org.in
- **ଟୋଲ୍ ଫ୍ରି ଫୋନ୍:** +91-1800-11-4949
- **ଟୋଲ୍ ଫ୍ରି ଫ୍ୟାକ୍ସ:** +91-1800-11-6969

ସୂଚନା ଡେସ୍କ

- **ଫୋନ୍:** +91-11-22902657

ପ୍ରଶିକ୍ଷଣ ଏବଂ ସଚେତନତା ଅଧିବେଶନରେ ଯୋଗଦେବା ପାଇଁ ଇମେଲ୍ କରନ୍ତୁ:

training@cert-in.org.in

ଆମକୁ ଅନୁସରଣ କରନ୍ତୁ

@IndianCERT

@cert_india

ସଚେତନତା ପୁସ୍ତିକାଗୁଡ଼ିକ

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

ସୁରକ୍ଷା ଉପକରଣଗୁଡ଼ିକ

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

SCAN ME!