CYBER SAFETY CAMPAIGN ODISHA - 2023

ADVISORY FOR HOUSEHOLD

1. How to be Cyber Safe

- Always have strong passwords with combination of letters, numbers, special characters.
- Do not reveal your password to anyone.
- Please do not save your passwords in web browsers.
- Be careful while sharing your personal information and photos on the internet.
- Be careful about suspicious emails, messages and do not click any link sent by them.
- Please do not respond to lucrative offers received by messages or email.
- Download software, apps and files from trusted sources only.
- Keep your computer, laptop, tablet, phone installed with latest software and security updates.

2. What are the precautions to be taken while using Social Media

- Keep your social media password strong and never share with anyone.
- If you think your password is compromised, change it immediately.
- Change your password periodically.
- Adjust the privacy settings on your social media profiles to control who can see your posts and personal information.
- Be cautious and verify the profile before accepting friend requests from unknown individuals.

@cybercopodisha

www.cybercrime.gov.in

Cyber Crime Help Line No :

1930

- As far as possible keep your profile locked so that it would be visible to your friends only.
- Never share your photo/video with anyone online.
- Do not answer video calls from unknown people.
- Immediately report to Facebook or Instagram, if you notice that your fake account has been created.
- Don't pay anyone if someone is asking money through social media messaging app (Facebook/Instagram/WhatsApp), before paying call the person and verify the genuineness.

3. How to ensure safety of your child in cyber space

- Please keep a watch over the smartphone and internet usage by your child.
- Please activate parental control and restricted/child mode over the smartphone of your child.
- Check their browsing history in between.
- Follow the social media account of your child and see what they post or share.
- Make the social media account of your child private.
- Never allow your children to play online games without your knowledge.
- Never allow children install any gaming application, that asks for money to play.
- Never allow children to save your Credit card/ Debit card/ UPI details in any game application.
- Never give your child ATM/Credit Card till he/she becomes an adult.
- Keep a watch on the time spent by your child on mobile, internet and social media.
- Brief your children about how to remain safe in cyber space and the social media precautions as given above.

4. What precautions are to be taken in online Financial Transactions

- Do not share OTP with any unknown person. OTP is a very secret thing which you only should use.
- Never provide personal information including your account numbers, Credit card, Debit card, UPI details to unknown persons.
- Immediately block the card and report to your bank in case of theft or loss.
- Always remember, you don't have to scan a QR code when receiving money.

5. Online Shopping Precautions

- Do not use public computers for online banking, shopping etc.
- Buy from trusted sources.
- Don't click on malicious pop-ups.
- Remember online shopping sites normally do not offer any prize.

6. KYC/PAN/Aadhar Updation Fraud

- Bank never ask through message or call to update Aadhar/ PAN/ KYC.
- Please do not entertain any SMS or call asking to update KYC. Simply delete the SMS and block the caller.
- Don't install remote applications which will create mirror image of your system at the fraudster's side.
- Please visit your bank or speak to the Manager and verify if there is a need to update your KYC

7. Search Engine Usage Fraud

- Be cautious while taking customer care number from google/any other search engine.
- It is better to go to original website and Use official website to get customer care number.

8. Job Frauds

- Never pay for an online job, it can be a fraud.
- Do not accept any lucrative part time job offer received through telegram/whatsapp.
- Never deposit money following the advice of any unknown person who assures you more income or premium membership etc.
- Never invest money as per the direction of unknown persons in crypto currency as they would be fake.
- Do not go by the opportunities found on search engines advertisement.

9. Loan App fraud

- Do not download any application to get any easy loan, please visit bank to apply for loan.
- Do not panic if the fraudster is sending your morphed nude photographs to your near and dears, that is their strategy to trap you financially.
- Do not repay loan with exorbitant interest amount to the online loan apps.

10. Matrimonial/ Gift Fraud

- Always do a background check of the prospective match both in social media or in matrimonial site.

- Ask enough questions. Do not share personal information.
- Whenever you make friends through online/ matrimony /social media don't trust their physical existence till you see that person on video couple of times that too without prior intimation.
- Be cautious while dealing with NRI profiles.
- Even in some cases they pretend to visit India to meet you but that can be a trap.

- They might offer you gift/ money/ valuable articles through parcel.
- From airport you may receive call that unauthorised articles and money have come from abroad.
- For disposal of the same, they will ask for money in the name of custom duties.
- Never accept transfer/ deposit money in return of gift as custom clearance.

11. Unknown Call-SIM Swap Fraud

- Now a days unknown call and links are coming through SMS/WhatsApp message.
- This may be for SIM swap, unknowingly you are giving consent to swap your sim card to other's name.
- By doing this, your bank account may be compromised and they may transfer the whole amount from your bank account.
- Other password can be compromised also.
- Please do not click any link sent by any unknown person.

12. Tower Installation fraud

- Mobile Service providers never ask for tower installation on private land.
- Never call anyone after going through any online/ news paper advertisement or SMS.
- Never pay anyone to install tower in your private land.

13. Online buying/selling fraud

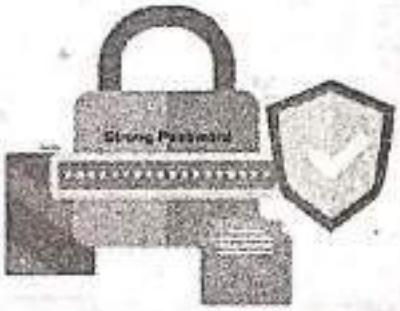
- Do not blindly trust any olx user.
- Do not get carried away on seeing products at unbelievably low price in OLX as it can be a fraud.
- Before buying any product from olx, please verify the user and have a one to one conversation.
- Don't click on any link if any olx user is sending the link through any UPI app.

ସାଇବର ସୁରକ୍ଷା ଅଭିଯାନ
ଓଡ଼ିଶା - ୨୦୨୩

ସାଧାରଣ ଲୋକଙ୍କ ପାଇଁ ପରାମର୍ଶ

୧. କିପରି ସାଇବର ଅପରାଧରୁ ସୁରକ୍ଷିତ ରହିବେ

- ଜଟିନ ପାସୱାର୍ଡ ବ୍ୟବହାର କରନ୍ତୁ । ଏଥିରେ ଅକ୍ଷର, ସଂଖ୍ୟା ଏବଂ ସ୍ପେଚିଆଲ କ୍ୟାରେକ୍ଟର୍ ବ୍ୟବହାର କରନ୍ତୁ ।
- ନିଜର ପାସୱାର୍ଡ କାହାକୁ ଦିଅନ୍ତୁ ନାହିଁ । କିମ୍ବା ଓ୍ୱେବ ବ୍ରାଉଜରରେ ପାସୱାର୍ଡ ସେଭ କରନ୍ତୁ ନାହିଁ ।
- ଜୌଣସି କାଗଜ ବା ଅନ୍ୟ ସ୍ଥାନରେ ୟୁଜର ଆଇଡି ବା ପାସୱାର୍ଡ ଲେଖି ରଖନ୍ତୁ ନାହିଁ ।
- ବ୍ୟକ୍ତିଗତ ତଥ୍ୟ ବା ଫଟୋ ଇଣ୍ଟରନେଟରେ ସେୟାର କରିବା ସମୟରେ ସତର୍କ ରୁହନ୍ତୁ ।
- ଇ-ମେଲ, ମେସେଜ ପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ ଏବଂ ଏଥିରେ ଥାଏଥିବା ଲିଙ୍କ ଉପରେ କ୍ଲିକ କରନ୍ତୁ ନାହିଁ ।
- ଅଫରଯୁକ୍ତ ମୋଲ ବା ମୋବେଇରର ଭରସା ଦିଅନ୍ତୁ ନାହିଁ ।
- କେବଳ ବିଶ୍ୱସ୍ତ ସୋର୍ସରୁ ହିଁ ସଫ୍ଟୱେୟାର, ଆପ୍ଲିକେସନ୍ କିମ୍ବା ଫାଇଲ ଡାଉନଲୋଡ୍ କରନ୍ତୁ ।
- କମ୍ପ୍ୟୁଟର, ଲାପଟପ୍, ଟାବଲେଟ୍, ଫୋନ୍ ଆଦିକୁ ଲାଟେଷ୍ଟ ସଫ୍ଟୱେୟାର ଏବଂ ସିକ୍ୟୁରିଟି ମାଧ୍ୟମରେ ଅପ୍‌ଡେଟ ରଖନ୍ତୁ ।



୨. ସୋସିଆଲ ମିଡ଼ିଆ ବ୍ୟବହାର କ୍ଷେତ୍ରରେ ସତର୍କତା

- ଜଟିନ ପାସୱାର୍ଡ ବ୍ୟବହାର କରନ୍ତୁ । ଏଥିରେ ଅକ୍ଷର, ସଂଖ୍ୟା ଏବଂ ସ୍ପେସିଆଲ କ୍ୟାରାକ୍ଟର ବ୍ୟବହାର କରନ୍ତୁ । ଜାହାଣିକୁ ନିଜର ପାସୱାର୍ଡ ଦିଅନ୍ତୁ ନାହିଁ ।
- ପାସୱାର୍ଡ ରିଜ୍ ହେବାର ଭୟ ଥିଲେ ଏହାକୁ ତୁରନ୍ତ ବଦଳାଇ ନିଅନ୍ତୁ ।
- ସମୟ ବ୍ୟବଧାନରେ ପାସୱାର୍ଡ ବଦଳାନ୍ତୁ ।
- ଆପଣଙ୍କ ସୋସିଆଲ ମିଡ଼ିଆ ଆକାଉଣ୍ଟରେ ଜେଉଁମାନେ ଆପଣଙ୍କ ପୋଷ୍ଟ ବା ବ୍ୟକ୍ତିଗତ ତଥ୍ୟ ଦେଖିପାରିବେ ସେ ନେଇ ପ୍ରାଇଭେସି ସେଟିଂ କରନ୍ତୁ ।
- ଲୋକଙ୍କ ଠାରୁ ଫ୍ରେଣ୍ଡ ରିକ୍ୱେଷ୍ଟ ଗ୍ରହଣ କରିବା ପୂର୍ବରୁ ତାଙ୍କ ପ୍ରୋଫାଇଲ ଉଲଟାଇରେ ଯାଞ୍ଚ କରିନିଅନ୍ତୁ ।

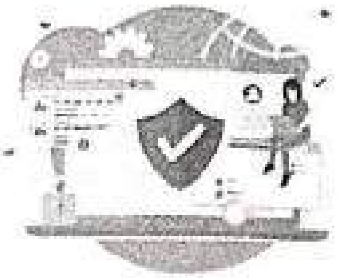
ସଚେତନ ହେବା, ସାଇବର ଅପରାଧ ରୋକିବା

www.cybercrime.gov.in @cybercopodisha

ସାଇବର ଅପରାଧ ସହାୟତା ନଂ
୧୯୩୦

- ଯେତେ ସମ୍ଭବ ନିଜ ପ୍ରୋଫାଇଲ୍ ଲକ୍ କରି ରଖନ୍ତୁ ଯଦ୍ୱାରା କେବଳ ଆପଣଙ୍କ ସୋସିଆଲ ମିଡିଆ ଫ୍ରେଣ୍ଡସ୍ ହିଁ ଆପଣଙ୍କ ବିଷୟରେ ଜାଣିପାରିବେ ।
- ଆପଣଙ୍କ ଫୋଟୋ ବା ଭିଡିଓ କଦାପି କାହାକୁ ପଠାନ୍ତୁ ନାହିଁ
- ଅଜଣା ନମ୍ବରରୁ ଭିଡିଓ କଲ ଆସୁଥିଲେ ଆଦୌ ତାହାର ଉତ୍ତର ଦିଅନ୍ତୁ ନାହିଁ
- ଫେସବୁକ୍ ବା ଇନଷ୍ଟାଗ୍ରାମରେ ଫେକ୍ ଆକାଉଣ୍ଟ ଆପଣଙ୍କ ନଜରକୁ ଆସିଲେ ତୁରନ୍ତ ଫେସବୁକ୍ ଓ ଇନଷ୍ଟାଗ୍ରାମକୁ ସେହି ଆକାଉଣ୍ଟ ପାଇଁ ରିପୋର୍ଟ କରନ୍ତୁ ।
- ଇନଷ୍ଟାଗ୍ରାମ ବା ହ୍ୱାଟସଆପରେ କେହି ଅର୍ଥ ମାଗୁଥିଲେ ଦିଅନ୍ତୁ ନାହିଁ । କଲ୍ କରି କିମ୍ବା ବ୍ୟକ୍ତିଗତ ଭାବେ ସାକ୍ଷାତ କରି ଜାଣିନିଅନ୍ତୁ ଏହାର କେତେ ସତ୍ୟାସତ୍ୟ ଅଛି ।

୩. ପିଲାଙ୍କୁ କିପରି ସାଇବର ଅପରାଧରୁ ସୁରକ୍ଷିତ ରଖିବେ



- ସ୍ମାର୍ଟଫୋନ ବା ଇଣ୍ଟରନେଟ୍ ବ୍ୟବହାର କରୁଥିଲେ ଆପଣ ତାଙ୍କ ଉପରେ ଦୃଷ୍ଟି ରଖନ୍ତୁ ।
- ବ୍ୟବହାର କରୁଥିବା ସ୍ମାର୍ଟ ଫୋନରେ ପାରେଣ୍ଟାଲ କଣ୍ଟ୍ରୋଲ, ଚାଇଲ୍ଡ ମୋଡ୍ ଆକ୍ଟିଭେଟ କରନ୍ତୁ ।
- ଇଣ୍ଟରନେଟରେ ସେମାନେ କେଉଁ ତଥ୍ୟ ଖୋଜୁଛନ୍ତି ବ୍ରାଉଜିଂ ହିଷ୍ଟ୍ରିରେ ଯାଞ୍ଚ କରନ୍ତୁ ।
- ସୋସିଆଲ ମିଡିଆ ଆକାଉଣ୍ଟକୁ ଫଲୋ କରି ଦେଖନ୍ତୁ ସେମାନେ କ'ଣ ସବୁ ପୋଷ୍ଟ କରୁଛନ୍ତି ବା ସେୟାର କରୁଛନ୍ତି ।
- ଆପଣଙ୍କ ଶିଶୁର ସୋସିଆଲ ମିଡିଆ ଆକାଉଣ୍ଟକୁ ପ୍ରାଇଭେଟ ରଖନ୍ତୁ ।
- ଅଜାଣତରେ ଆପଣଙ୍କ ପିଲା ଯେପରି ଅନଲାଇନ ଗେମ୍ ନଖେଳନ୍ତି ସେଥିପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ ।
- ଅର୍ଥ ମାଗୁଥିବା ଗେମିଂ ଆପ୍ଲିକେସନ ଇନଷ୍ଟଲ କରିବାରୁ ନିଜ ପିଲାଙ୍କୁ ନିବୃତ୍ତ ରଖନ୍ତୁ ।
- ଶିଶୁ ଯେପରି କୌଣସି ଗେମିଙ୍ଗ ଆପ୍ଲିକେସନରେ ଆପଣଙ୍କ କ୍ରେଡିଟ କାର୍ଡ/ ଡେବିଟ କାର୍ଡ / ୟୁପିଆଇ ତଥ୍ୟ ସେଭ ନକରନ୍ତି ସେଥିପ୍ରତି ଧ୍ୟାନ ଦିଅନ୍ତୁ ।
- ଶିଶୁ ସାବାଳକ ନହେବା ପର୍ଯ୍ୟନ୍ତ ତାଙ୍କୁ ଏଟିଏମ କିମ୍ବା କ୍ରେଡିଟ କାର୍ଡ ଦିଅନ୍ତୁ ନାହିଁ ।
- ଶିଶୁ କେତେ ସମୟ ମୋବାଇଲ ବା ଇଣ୍ଟରନେଟରେ ସମୟ ଦେଉଛନ୍ତି ସେଥିପ୍ରତି ନଜର ରଖନ୍ତୁ ।
- ସୁରକ୍ଷା ନେଇ ପିଲାମାନଙ୍କୁ ସଚେତନ କରାନ୍ତୁ ।

୪. ଆର୍ଥିକ କାରବାର ସମୟରେ ସତର୍କ ରୁହନ୍ତୁ

- କୌଣସି ଅଜଣା ବ୍ୟକ୍ତିଙ୍କ ସହ ବ୍ୟାଙ୍କର ତଥ୍ୟ ସେୟାର କରନ୍ତୁ ନାହିଁ ।
- କ୍ରେଡିଟ୍ କାର୍ଡ, ଡେବିଟ କାର୍ଡ, ୟୁପିଆଇ ତଥ୍ୟ ଭଳି ବ୍ୟକ୍ତିଗତ ସୂଚନା ଅଜଣା ବ୍ୟକ୍ତିଙ୍କୁ କଦାପି ଦିଅନ୍ତୁ ନାହିଁ ।
- କ୍ରେଡିଟ୍ କାର୍ଡ, ଡେବିଟ କାର୍ଡ ଆଦି ହଜିଯାଇଥିଲେ ତୁରନ୍ତ ବ୍ୟାଙ୍କକୁ ସୂଚିତ କରିବା ସହ କାର୍ଡ ବ୍ଲକ କରନ୍ତୁ ।

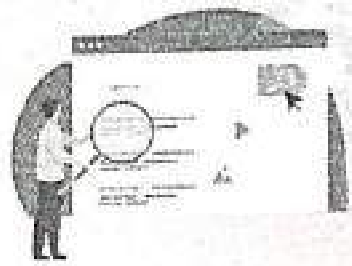
୫. ଅନଲାଇନ ସପିଂରେ ସତର୍କତା

- ବ୍ୟାଙ୍କିଙ୍ଗ ବା ସପିଂ କରୁଥିଲେ ସର୍ବସାଧାରଣ କମ୍ପ୍ୟୁଟର ବ୍ୟବହାର କରନ୍ତୁ ନାହିଁ ।
- ଅଥେଣ୍ଟିକ୍ ସାଇଟ ବା ପୋର୍ଟାଲରୁ କିଣାକିଣି କରନ୍ତୁ ।
- ଅଜଣା ଲିଙ୍କରେ କ୍ଲିକ କରନ୍ତୁ ନାହିଁ ।
- ଅନଲାଇନ ସପିଂ ସାଇଟ ଗୁଡ଼ିକ ସାଧାରଣତଃ କୌଣସି ଅଫର ବା ଉପହାର ଦିଅନ୍ତି ନାହିଁ ।

୬. କେୱାଇସି/ଆଧାର/ପ୍ୟାନ ସମ୍ପର୍କିତ ଠକେଇ

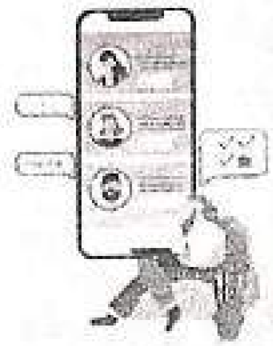
- କେୱାଇସି ଅପଡେଟ କରିବା ପାଇଁ ବ୍ୟାଙ୍କ କାହାକୁ କଲ ବା ମେସେଜ କରେ ନାହିଁ ।
- କେୱାଇସି ଅପଡେଟ ପାଇଁ ଏସ୍‌ଏମ୍‌ଏସ୍ ଆସୁଥିବା ନମ୍ବରରେ ଉତ୍ତର ଦିଅନ୍ତୁ ନାହିଁ ବରଂ କଲ ବା ମେସେଜ କରୁଥିବା ନମ୍ବରକୁ ବ୍ଲକ କରିଦିଅନ୍ତୁ ।
- କୌଣସି ରିମୋଟ୍ ଆପ୍ଲିକେସନ୍ ଇନ୍‌ଷ୍ଟଲ୍ କରନ୍ତୁ ନାହିଁ, ଏହା କରିବା ଦ୍ୱାରା ସାଇବର ଅପରାଧି ଆପଣଙ୍କ ସିଷ୍ଟମର ମିରର ଇମେଜ (ପ୍ରତିବିମ୍ବ) ସୃଷ୍ଟି କରିଥାଏ । ଫଳରେ ଆପଣଙ୍କ ତଥ୍ୟ କମ୍ପ୍ରୋମାଇଜ୍ ହୋଇପାରେ ।
- ଏପରି ମେସେଜ ପାଇଥିଲେ ନିଜ ବ୍ୟାଙ୍କକୁ ଯାଇ ପଚାରି ବୁଝନ୍ତୁ ଏବଂ ଆବଶ୍ୟକ ଥିଲେ ବ୍ୟାଙ୍କରେ କେୱାଇସି ଅପଡେଟ କରନ୍ତୁ ।

୭. ସର୍ଚ୍ଚ ଇଞ୍ଜିନର ବ୍ୟବହାର ଠକେଇ



- କୌଣସି କଷ୍ଟମର୍ କେୟାର ନମ୍ବର ସର୍ଚ୍ଚ ଇଞ୍ଜିନ୍‌ର ବ୍ୟବହାର କରି ଖୋଜନ୍ତୁ ନାହିଁ ।
- ଅରିଜିନାଲ୍ ଏବଂ ଅଫିସିଆଲ ୱେବସାଇଟରୁ କଷ୍ଟୋମର କେୟାର ନମ୍ବର ନେବା ଅପେକ୍ଷାକୃତ ସୁରକ୍ଷିତ ହୋଇଥାଏ ।

୮. ନିଯୁକ୍ତି ଠକେଇ



- କୌଣସି ଅନ୍‌ଲାଇନ୍‌ରେ ପାଉଥିବା ଚାକିରି ପାଇଁ ପଇସା ଦିଅନ୍ତୁ ନାହିଁ, ଆପଣ ଠକେଇରେ ପଡ଼ିପାରନ୍ତି ।
- ଟେଲିଗ୍ରାମ୍ ଏବଂ ହ୍ୱାଟସଆପରେ କୌଣସି ଲୋଭନୀୟ ପାର୍ଟଟାଇମ ନିଯୁକ୍ତି ଅଫର ଗ୍ରହଣ କରନ୍ତୁ ନାହିଁ ।
- ରୋଜଗାର ପାଇଁ ଅନଲାଇନରେ କେହି ଅଜଣା ବ୍ୟକ୍ତି ଟଙ୍କା ଦେବା ପାଇଁ ପରାମର୍ଶ ଦେଉଥିଲେ ଟଙ୍କା ଦିଅନ୍ତୁ ନାହିଁ
- କୌଣସି ଲୋକର କଥାରେ ପଡି କ୍ରିପ୍ଟୋ କରେନ୍ସିରେ ଟଙ୍କା ଜମା କରନ୍ତୁ ନାହିଁ ।
- ସର୍ଚ୍ଚ ଇଞ୍ଜିନର ବିଜ୍ଞାପନ ଦ୍ୱାରା ପାଉଥିବା ନିଯୁକ୍ତି ଉପରେ ବିଶ୍ୱାସ କରନ୍ତୁ ନାହିଁ ।
- ଇଣ୍ଟରଭ୍ୟୁ ପାଇଁ ଅର୍ଥ ଦେବାକୁ ପଡୁଥିଲେ ସେଠାରୁ ନିବୃତ୍ତ ରୁହନ୍ତୁ ।

୯. ଲୋନ ଆପ ଠକେଇ

- ଲୋନ୍ ପାଇବା ପାଇଁ କୌଣସି ଲୋନ ଆପ୍ ବ୍ୟବହାର କରନ୍ତୁ ନାହିଁ ବରଂ ନିଜସ୍ୱ ବ୍ୟାଙ୍କ ସହ ସମ୍ପର୍କ କରନ୍ତୁ ।
- ଯଦି କେହି ଲୋନ ରିପେମେଣ୍ଟ ପାଇଁ ଆପଣଙ୍କ ଅଶ୍ଳୀଳ ଫଟୋ ଆପଣଙ୍କ ସମ୍ପର୍କୀୟଙ୍କୁ ପଠାଉଛନ୍ତି ଆଦୌ ଭୟ କରନ୍ତୁ ନାହିଁ । ଆପଣଙ୍କ ଠାରୁ ଟଙ୍କା ନେବା ପାଇଁ ସେମାନଙ୍କର ଏହା ଏକ ଅଭିନବ ଉପାୟ ।
- ଲୋନ ରିପେମେଣ୍ଟ ପାଇଁ ଅତିରିକ୍ତ ସୁଧ ବା ଅର୍ଥ ଲୋନ ଆପ୍‌ରେ ଦିଅନ୍ତୁ ନାହିଁ ।

୧୦. ମାଟ୍ରିମୋନିଆଲ ବା ଉପହାର ଠକେଇ

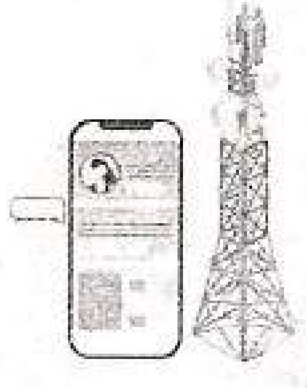
- ସୋସିଆଲ ମିଡ଼ିଆ ବା ମାଟ୍ରିମୋନିଆଲ ସାଇଟରେ ଜୀବନସାଥୀ ଖୋଜୁଥିଲେ ସର୍ବଦା ସତ୍ୟାସତ୍ୟ ଯାଞ୍ଚ କରନ୍ତୁ ।
- ଆପଣଙ୍କର ଅଜଣା ବନ୍ଧୁଙ୍କୁ ପ୍ରଶ୍ନ ପଚାରି ସନ୍ଦେହ ଦୂର କରନ୍ତୁ, ଏହା ପୂର୍ବରୁ ନିଜର ବ୍ୟକ୍ତିଗତ ସୂଚନା ଦିଅନ୍ତୁ ନାହିଁ ।

- ସୋସିଆଲ ମିଡିଆ ବା ମାଟ୍ରିମୋନିଆଲ ସାଇଟରେ ବନ୍ଧୁତ୍ୱ କରୁଥିଲେ ଅନ୍ଧ ଭାବରେ ବିଶ୍ୱାସ କରନ୍ତୁ ନାହିଁ ।
- ଉକ୍ତ ବ୍ୟକ୍ତିଙ୍କୁ ସର୍ବସାଧାରଣ ସ୍ଥାନରେ ହିଁ ଦେଖା କରିବାକୁ କୁହନ୍ତୁ ।
- NRI ବର ଚୟନବେଳରେ ଅଧିକ ସତର୍କତା ଅବଲମ୍ବନ କରିବା ଜରୁରୀ ।
- କେତେକ ମାମଲାରେ ସେ ଆପଣଙ୍କୁ ଭେଟିବାକୁ ଭାରତ ଆସିବା ନେଇ ଛଳନା କରିପାରନ୍ତି । ଆପଣଙ୍କୁ ଠକିବା ପାଇଁ ଏହା ଏକ ଚାଲ ହୋଇପାରେ । ଏଥିପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ ।
- ଆପଣଙ୍କୁ ଜାଲରେ ଫସାଇବା ପାଇଁ କିଛି ଉପହାର/ଟଙ୍କା/ ମୂଲ୍ୟବାନ ଜିନିଷ ପାର୍ସଲ ଆକାରରେ ଦେଇପାରନ୍ତି ।
- ଆପଣଙ୍କ ପାଇଁ ପାର୍ସଲ ଆସିଛି କହି ଏୟାରପୋର୍ଟରୁ କଲ ମଧ୍ୟ ଆସିପାରେ, ତାହାକୁ ଆପଣ ବିଶ୍ୱାସ କରନ୍ତୁ ନାହିଁ ।
- ଉପହାର ବଦଳରେ ଆପଣଙ୍କୁ ଅର୍ଥ ପାଇଁ ଦାବି କରାଯାଇପାରେ ।
- ଉପହାର ବଦଳରେ ଆଦୌ ଟଙ୍କା ଟ୍ରାନ୍ସଫର ବା ଡିପୋଜିଟ କରନ୍ତୁ ନାହିଁ ।

୧୧. ଅଜଣା କଲ୍-ସିମ ସ୍ୱାପ ଠକେଇ

- ଯଦି ବାରି ବାରି ଅଜଣା ନମ୍ବରରୁ ଅନେକ କଲ ବା ଲିଙ୍କ ଏସଏମଏସ / ହ୍ୱାଟସଆପ ମେସେଜ ମାଧ୍ୟମରେ ଆସୁଛି ।
- ଏହା ଦ୍ୱାରା ଆପଣଙ୍କ ସିମ ଅନ୍ୟ ନାମରେ ଟ୍ରାନ୍ସଫର ହୋଇପାରେ । ଆପଣଙ୍କ ଅଜାଣତରେ ଆପଣ ଏଥିପାଇଁ ଅନୁମତି ଦେଇଥାନ୍ତି ।
- ଏହା କରିବା ଦ୍ୱାରା ଆପଣଙ୍କ ବ୍ୟାଙ୍କ ଆକାଉଣ୍ଟରେ ଥିବା ସମସ୍ତ ଅର୍ଥ ସେମାନେ ନିଜ ଆକାଉଣ୍ଟକୁ ଟ୍ରାନ୍ସଫର କରିନିଅନ୍ତି ।
- ଆପଣଙ୍କର ଅନ୍ୟ ପାସୱାର୍ଡ ମଧ୍ୟ ସେମାନେ ଜାଣିଯାଇ ପାରନ୍ତି ।
- କୌଣସି ଅଜଣା ବ୍ୟକ୍ତି ପଠାଇଥିବା ଲିଙ୍କ ଉପରେ କ୍ଲିକ କରନ୍ତୁ ନାହିଁ ।

୧୨. ଟାୱାର ବସେଇବା ନାମରେ ଠକେଇ



- ମୋବାଇଲ୍ ସେବା ପ୍ରଦାନକାରୀ ସଂସ୍ଥା ଘରୋଇ ଜମିରେ ଟାୱାର ବସାଇବା ପାଇଁ କୌଣସି ବ୍ୟକ୍ତିଙ୍କୁ ସିଧାସଳଖ ପଚାରନ୍ତି ନାହିଁ । ତେଣୁ ଏଥିପ୍ରତି ସତର୍କ ରୁହନ୍ତୁ ।
- କୌଣସି ଖବରକାଗଜ ବା ଏସଏମଏସରେ ଏପରି ବିଜ୍ଞାପନ ଦେଖିଲେ ଆଦୌ ଉକ୍ତ ନମ୍ବରରେ କଲ କରନ୍ତୁ ନାହିଁ ।
- ଘରୋଇ ଜମିରେ ମୋବାଇଲ ଟାୱାର ବସାଇବା ପାଇଁ କାହାରିକୁ ଅର୍ଥ ଦିଅନ୍ତୁ ନାହିଁ ।

୧୩. ଓଏଲଏକ୍ସ ଠକେଇ

- ଓଏଲଏକ୍ସ ବ୍ୟବହାରକାରୀଙ୍କୁ ଅନ୍ଧ ଭଳି ଭରସା କରନ୍ତୁ ନାହିଁ ।
- କୌଣସି ଜିନିଷ ଆବଶ୍ୟକତାଠାରୁ ଅଧିକ ଶସ୍ତାରେ ମିଳୁଥିଲେ ସେଥିରେ ବିଶ୍ୱାସ କରନ୍ତୁ ନାହିଁ । ଏହାଦ୍ୱାରା ଆପଣ ଠକେଇରେ ପଡ଼ିପାରନ୍ତି ।
- କୌଣସି ଜିନିଷ କିଣୁଥିଲେ ଅର୍ଥ ଦେବା ପୂର୍ବରୁ ବିକ୍ରେତାଙ୍କ ସହ ସାମନା ସାମନି କଥା ହୁଅନ୍ତୁ ଏବଂ ଜିନିଷର ସତ୍ୟାସତ୍ୟ ବିଷୟରେ ଭଲରେ ଯାଞ୍ଚ କରିନିଅନ୍ତୁ ।
- ଯଦି କୌଣସି ଓଏଲଏକ୍ସ ୟୁଜର କୌଣସି ୟୁପିଆଇ ଆପ ମାଧ୍ୟମରେ ଲିଙ୍କ ପଠାଉଥିଲେ ସେଥିରେ କ୍ଲିକ କରନ୍ତୁ ନାହିଁ ।