HEALTHY DIGITAL CHILDHOOD ALLIANCE

Tips for Parents: Talking to Kids About Social Engineering

1. **Start Early and Keep It Simple**
   Talk about what social engineering is in everyday language, like people trying to trick them online or in real life. Use simple examples, just like the story about Lila below.
2. **Make It a Conversation, Not a Lecture**
   Encourage your child to ask questions and share any strange or suspicious messages they get. Keep the conversation open and judgment-free, so they feel safe coming to you.
3. **Set Clear Rules About Sharing Information**
   Explain why passwords, addresses, and phone numbers are private. Teach kids never to share these without checking with a trusted adult first.
4. **Use Real-Life Scenarios**
   Help kids recognize common tactics, like someone pretending to be a friend, offering prizes, or trying to rush them. Role-play situations where they say “No” or ask for help.
5. **Use Parental Controls Wisely**
   Use monitoring tools to keep an eye on your child’s online activity, but don’t rely on them alone. Combine controls with good communication.
6. **Teach Them to Trust Their Instincts**
   If something feels off or too good to be true, it probably is. Encourage kids to stop, think, and talk to a grown-up before responding.
7. **Be a Good Digital Role Model**
   Show your child how you stay safe online. Practice cautious clicking, privacy settings, and strong passwords visibly.
8. **Stay Updated Together**
   Online threats change fast. Keep learning with your child about new scams and tricks.

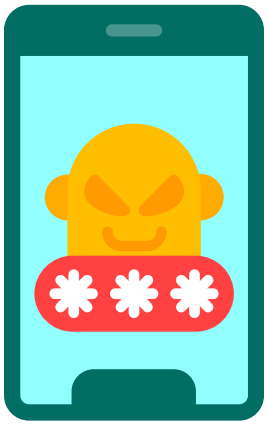
With awareness, rules, and a healthy dose of “trust but verify,” you can help your child build strong defences against social engineering, and become a smarter, safer digital citizen.

HEALTHY DIGITAL CHILDHOOD ALLIANCE

Lila and the Trickster's Game

Lila loved playing games and chatting with her friends online. One day, while playing a new game, she got a message from someone who said, "Hey Lila! I'm your friend Max's cousin. Max told me you're great at this game! Can you give me your password so I can help you win?"

Lila paused. She thought, "Wait, why would Max's cousin need my password? That sounds weird." This was a trick called social engineering, someone pretending to be a friend or someone she trusts to get secret information.



Social engineers are sneaky. They might send messages that say:

- "You've won a prize! Just give me your password to claim it."
- "Your account is about to be deleted, please send your login info right now!"
- "I'm a new friend, give me your address and phone number so we can meet."

People like Lila can stay safe by asking questions like:

- “How do you know Max’s cousin?”
- “Why do you need my password?”
- Always telling a parent or trusted adult before sharing anything personal.

Remember, real friends never ask for your password or personal details. If someone does, it’s okay to just say **“No”** and tell a grown-up you trust.

Home - Healthy Digital Childhood Alliance