SOCIAL MEDIA

Staying Secure in a Connected World

The average user spends over two hours a day on social media.
Discover some of the global risks and what you can do to stay safe.

Think before you CLICK!

Julie receives a message offering a “special version” of her favorite app. She clicks the link, enters her credentials, and installs the software. **Oh no!** Julie just got phished! Now the bad guys have her user info and complete access to her device.

JULIE

Have a strong security mindset:

- Never trust unexpected messages.
- Don’t click unexpected links.
- Only download and install software from verified sources.
- If it sounds too good to be true, it probably is.

MARK

Think before you SHARE!

Mark recently live-streamed a party from the office. **Oh no!** He never adjusted the security settings and broadcast proprietary information to the entire world. Also, since geotagging was still on, the bad guys know the time and location of his every picture and post and can easily target him.

Have a strong security mindset:

- Don’t assume default security settings protect you.
- Don’t give away sensitive or confidential information.
- Review and update security and privacy settings quarterly.
- Turn off geotagging to keep location information private.
- Only share with intended viewers.

Think before you CONNECT!

Tim accepts all connection requests. He recently connected with his CEO and has been sharing proprietary information using private messages. **Oh no!** Tim is the victim of a fake profile, which bad guys use to gain information and harm organizations.

TIM

Have a strong security mindset:

- Don’t blindly accept connection requests.
- Don’t assume the connection is real.
- Don’t use social media to send sensitive information.
- If a request seems suspicious, verify by contacting the person directly.
- Periodically review and remove unnecessary connections.

Review and follow your organization’s social media and security policies!

KnowBe4
Human error. Conquered.