# KEEPING CYBER SAFE IN A VIRTUAL WORKPLACE

REVEALRISK
SECURE YOUR BUSINESS

## KNOW YOUR INFORMATION

- Protect your personal and professional data by knowing what is sensitive and handling it properly.
- Do not give out sensitive personal or company data over social, text, email, or IM channels unless you can verify the receiver.

## BE SMART WITH YOUR DATA

- Only use approved file transfer, chat, and meetings tools for company business.
- Install software updates and back up your files.

## PROTECT YOUR ENVIRONMENT

- Use strong passwords and multi-factor authentication wherever you can and don't reuse passwords between work and personal accounts.
- Only use approved devices for work. Unapproved devices may not have adequate protection for sensitive company data.

## BEWARE OF SCAMS AND ATTACKERS

- Don't fall for promised miracle cures, COVID-19 test offers, or virus maps. Attackers read the news and incorporate it into their attacks.
- Verify unusual requests before taking actions such as wire transfers, emailing sensitive documents, or making purchases.

## LEARN AND ADAPT

- Take time to review remote workplace guidance from your corporate security team, especially if you're an infrequent teleworker.
- Don't forget to take breaks to recharge your focus. Significant change can cause fatigue and disrupt your normal productive rhythms.

## COMMUNICATE SMARTLY

- Have important phone numbers handy (critical team members, HR, IT, Security) - increased remote workers may stress the technology and create connectivity challenges.
- Alert your corporate IT / security team of any scams, phish, or other security events that happen while working remotely - just as you would in the office!