# БЕЗОПАСНОСТЬ В ОНЛАЙНОВОЙ СРЕДЕ С САНГО

## ГЛОССАРИЙ

**Фишинг:** фишинг – это кибератака, направленная на похищение персональных данных и осуществляемая путем размещения в сообщениях электронной почты поддельных ссылок, которые позволяют украсть ваш пароль или установить файл с вредоносным программным обеспечением.
**Вредоносное программное обеспечение:** программа, наносящая вред электронному устройству (компьютер, планшет, смартфон).
**Родительский контроль:** инструменты, позволяющие защитить детей от существующих в онлайновой среде угроз путем предотвращения потенциально опасных действий.

## ПЕРСОНАЛЬНЫЕ ДАННЫЕ

- Пользуясь интернетом, мы не осознаем, какой объем персональных данных мы передаем и каким образом другие могут использовать такие данные без нашего разрешения.
- **Никогда не делитесь** в интернете информацией о своем **пароле, домашнем адресе, номере телефона или дне рождения**. В то же время информация о ваших увлечениях также является конфиденциальной! Следите за тем, какие фотографии и видеоматериалы вы публикуете.
- **Помните: в интернете нет ничего, что могло бы оставаться полностью конфиденциальным!**

## ПРИЛОЖЕНИЯ

- Приложениями **фиксируется ряд персональных данных, таких как ваши контакты и местоположение, что позволяет людям со злыми намерениями** определить, где вы находитесь при использовании вами соответствующего приложения.
- Прежде чем покупать приложения или открывать новые уровни в играх, **обязательно расскажите о своих планах кому-нибудь из взрослых**, чтобы избежать нежелательных ситуаций.
- Используя приложения и посещая веб-сайты, соответствующие вашему возрасту, **играйте только с теми друзьями, которых вы знаете лично**.

## СОЦИАЛЬНЫЕ СЕТИ

- **Социальные сети** – это предназначенные для поддержания связи с друзьями инструменты, которые таят в себе множество угроз. В принципе создать **поддельный профиль** очень просто: будьте осторожны, поскольку **вы не представляете, кто может скрываться** под именем пользователя!
- Вы можете столкнуться не только с людьми со злыми намерениями, но и с **контентом, не соответствующим вашему возрасту**, например фото- или видеоматериалами, из-за которых **вы можете почувствовать себя неловко**.

## УГРОЗЫ

- Кража данных
- Кража идентичности
- Фишинг
- Просмотр фото- и видеоматериалов, не соответствующих вашему возрасту
- Благодаря включенной функции геолокации, приложения всегда "знают", где вы находитесь
- Ваш личный контент может оказаться в чужих руках без вашего разрешения

## КАКИМ ОБРАЗОМ ВЫ МОЖЕТЕ ЗАЩИТИТЬ СЕБЯ В ОНЛАЙНОВОЙ СРЕДЕ?

Когда вы не пользуетесь своим устройством, обязательно блокируйте его с помощью длинного, сложного и никому неизвестного пароля, с тем чтобы защитить свои учетные записи.

Установите настройки "закрытого" профиля и никогда и никому не сообщайте свои персональные данные; если необходимо, используйте для этих целей псевдоним.

Убедитесь, что вы знаете друзей, с которыми общаетесь в чатах и социальных сетях: обменивайтесь только тем контентом, который позволяет вам чувствовать себя комфортно.

Получив запрос или контент, из-за которого вы чувствуете себя неловко, или увидев что-либо, не соответствующее вашему возрасту, сообщите об этом кому-нибудь из взрослых.

Попросите кого-нибудь из взрослых, которым вы доверяете, установить режим родительского контроля на используемых вами устройствах.

## ЗНАЛИ ЛИ ВЫ, ЧТО...

Ваши персональные данные есть даже в вашем смартфоне, поэтому всегда блокируйте его и не оставляйте его без присмотра!

Оставайтесь с нами и следите за новостями на веб-сайтах www.itu-cop-guidelines.com и www.itu.int/cop

eni Deloitte. ITU