GROUP IB

ПРАВИЛА ВЫЖИВАНИЯ В ЦИФРОВОМ МИРЕ

Киберпространство — это особая цифровая среда, где полезное и интересное соседствует с опасностью и риском. Чтобы пользоваться интернетом безопасно, важно соблюдать базовые правила.

Безопасность устройств

- Регулярно обновляй операционную систему и приложения на смартфоне, планшете и персональном компьютере.
- Устанавливай приложения только из официальных источников (App Store, Google Play и Windows Market).
- Для каждого аккаунта используй индивидуальный пароль, который рекомендуется менять раз в три месяца. Роутера это тоже касается.
- Обязательно делай резервные копии важной информации.
- Всегда блокируй свои устройства (ПК, смартфон, планшет), когда не работаешь с ними.

Фишинг

- Помни, что злоумышленники постоянно придумывают новые правдоподобные сценарии, чтобы обмануть тебя — заставить открыть файл, перейти по ссылке или ввести персональные данные на мошеннической странице.
- Всегда внимательно проверяй адресата, от имени которого тебе пришло сообщение в электронной почте. Если возникли сомнения, лучше позвонить или другим способом связаться с человеком, от которого пришло письмо, чтобы убедиться, что это не мошенник.
- Не открывай подозрительные ссылки, файлы от незнакомцев в почте и в социальных сетях.
- Если тебе звонят из банка и просят выполнить какое-то подозрительное действие или раскрыть данные, сразу положи трубку и перезвони в банк по номеру телефона, указанному на сайте или на оборотной стороне банковской карты.

Безопасность в соцсетях

- Никогда не размещай в соцсетях данные паспорта, банковской карты или других документов, содержащих твои персональные данные.
- Не добавляй в друзья неизвестных тебе людей и закрой свой профиль от незнакомцев.
- Не хвастайся дорогими покупками в интернете и не раскрывай незнакомцам подробности о своей семье и семейном бюджете.
- Не выкладывай в соцсети фотографии родителей, родственников, близких и знакомых без их согласия.

Кибербуллинг и травля в интернете

- Если кто-то оскорбляет и провоцирует тебя в сети, сохраняй спокойствие и не ведись на провокацию.
- Сразу прекрати общение с этим человеком, заблокируй его и сообщи родителям или взрослому, которому доверяешь.

Управление «К»
МВД Республики Беларусь

01 НАДЕЖНЫЕ ПАРОЛИ

02 БЕЗОПАСНЫЙ WI-FI

03 БРАУЗЕРЫ И САЙТЫ

04 ЗАЩИТА ОНЛАЙН-БАНКИНГА

05 ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ

06 БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ

GROUP-IB

6 правил информационной безопасности

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕР-ПРЕСТУПНИКА

GROUP-IB

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам и менять их каждые 3 месяца
+ Использовать сложные пароли: минимум 12 символов, одновременно цифры, строчные и прописные буквы, знаки пунктуации
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

– Использовать повторения символов
– Хранить пароли на бумажных носителях
– Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
– Сохранять пароль автоматически в браузере
– Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

НЕОБХОДИМО:

+ Отключить общий доступ к вашей Wi-Fi сети и использовать надежный пароль к ней
+ Обновить прошивку роутера и сменить пароль к административной панели
+ Запретить автоматическое подключение своих устройств к открытым Wi-Fi точкам

НЕ РЕКОМЕНДУЕТСЯ:

– Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

БРАУЗЕРЫ И САЙТЫ 03

НЕОБХОДИМО:

+ Обновлять браузер и плагины
+ Использовать VPN

НЕ РЕКОМЕНДУЕТСЯ:

– Переходить по непроверенным ссылкам
– Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)
– Сохранять персональные данные в браузере

ЗАЩИТА ОНЛАЙН-БАНКИНГА 04

НЕОБХОДИМО:

+ Хранить в тайне пин-код карты и другие банковские данные
+ Прикрывать ладонью клавиатуру при вводе пин-кода
+ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
+ Использовать лимиты на максимальные суммы онлайн-операций
+ Скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

НЕ РЕКОМЕНДУЕТСЯ:

– Хранить пин-код вместе с карточкой/на карточке
– Сообщать CVV-код или отправлять его фото
– Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), логин и пароль для доступа к системе интернет-банкинга
– Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации и т.д.

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

НЕОБХОДИМО:

+ Устанавливать приложения только из официальных магазинов
+ Обращать внимание, к каким функциям устройства приложение запрашивает доступ
+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

НЕ РЕКОМЕНДУЕТСЯ:

– Размещать персональную и контактную информацию о себе в открытом доступе
– Указывать геолокацию на фото в постах
– Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
– Употреблять ненормативную лексику при общении
– Устанавливать приложения с низким рейтингом и негативными отзывами

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 06

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать разную почту для переписок и для регистраций на сайтах
+ Использовать спам-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

– Реагировать на письма от неизвестного отправителя – скорее всего это спам или мошенники
– Открывать подозрительное вложение к письму – сначала позвоните отправителю и узнайте, что это за файл