

## Для доведения работникам организации

Киберпреступность является международной проблемой. Подобные преступления совершаются, как правило, транснациональными организованными преступными группами, члены которых при помощи сети Интернет, легко пересекают виртуальные границы и совершают преступления в отношении иностранных граждан и граждан Республики Беларусь.

Для того чтобы не стать жертвой киберпреступника необходимо соблюдать следующие простые правила:

### **ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ**

#### **Необходимо:**

- + Хранить в тайне пин-код карты
- + Прикрывать ладонью клавиатуру при вводе пин-кода
- + Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
- + Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций
- + Скрыть CCV-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» доступа к системе «Интернет-банкинг»
- Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.

### **НАДЕЖНЫЕ ПАРОЛИ**

#### **Необходимо:**

- + Создавать персональные (уникальные) пароли к разным сервисам
- + Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
- + 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 пароли автоматически в браузере
- Использовать биографическую информацию в пароле

### **ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ**

#### **Необходимо:**

- + Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

Не рекомендуется:

- Переходить по непроверенным ссылкам
- Вводить информацию на сайтах, если соединение не защищено

**БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ**

Необходимо:

- + Подключить двухфакторную аутентификацию
- + Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
- + 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, узнайте, что это за файл.

**ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦИАЛЬНЫХ СЕТЕЙ И МЕССЕНДЖЕРОВ**

Необходимо:

- + Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
- + Обращать внимание, к каким функциям гаджета 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
- Использовать указание геолокации на фото в постах
- Отвечать на обидные выражения и агрессию в социальных сетях – лучше напишите об этом администратору ресурса
- Употреблять ненормативную лексику при общении
- Устанавливать приложения с низким рейтингом и отрицательными отзывами

**УПК КМ УВД Гомельского облисполкома**