Руководителям предприятий,
организаций

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.

В настоящее время состояние информационной сферы в Республике Беларусь характеризуется высоким уровнем доступа населения страны к массовой информации. Количество национальных средств массовой информации и интернет-ресурсов неуклонно увеличивается. Белорусское информационное пространство открыто для активной работы иностранных СМИ и интернет-ресурсов. В стране ежегодно увеличивается пропускная способность внешних каналов доступа в сеть Интернет, количество интернет-пользователей, абонентов сетей электросвязи, держателей банковских платежных карт.

Сегодня спектр преступлений в сфере высоких технологий значительно расширился и может коснуться любого гражданина или организации не зависимо от формы собственности. Наиболее распространенными являются: хищение денежных средств при помощи реквизитов банковских платежных карт, внесение заведомо ложных сведений в компьютерную систему с целью незаконного получения кредитов либо сокрытия фактов хищений, уничтожение компьютерной информации, незаконное копирование или завладение информацией, хранящейся в компьютерной системе, взлом почтовых ящиков и дальнейший незаконный доступ к информации. Подобных примеров можно привести очень много.

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

БЕЗОПАСНЫЙ WI-FI

Необходимо:
+ Отключить общий доступ к своей WI-FI точке, даже если у вас «безлимитный» Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей WI-FI точке
+ Деактивировать 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.

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:

- Не 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

ОРПСВТ КМ УВД Гомельского облисполкома