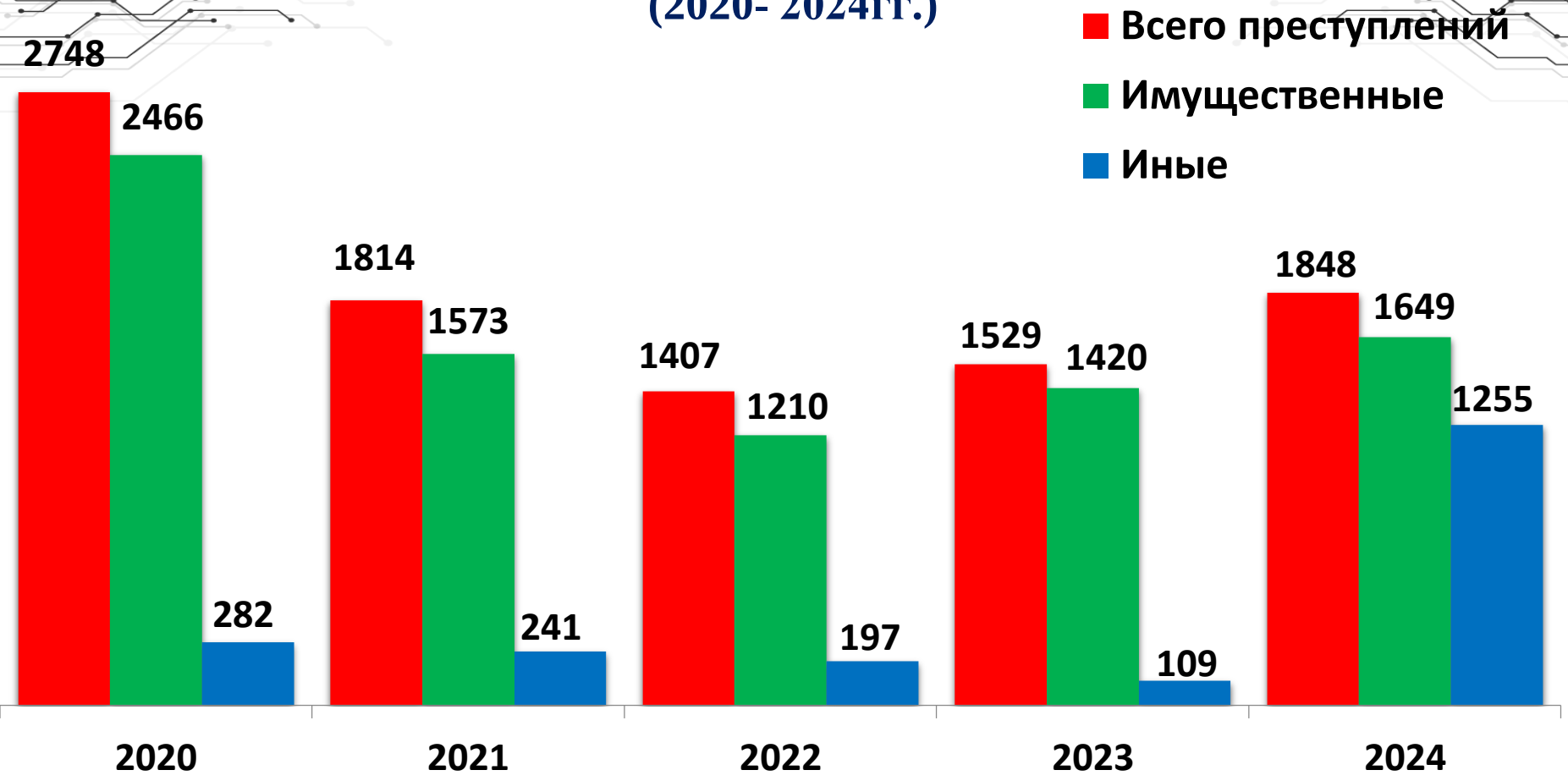
Актуальные способы совершения киберпреступлений. Безопасность в сети Интернет.

Матяс Артем Геннадьевич

Начальник УПК КМ
УВД Гродненского облисполкома

Динамика киберпреступности (2020- 2024гг.)



Актуальные виды преступлений

- **Завладение денежными средствами с карт-счета с использованием вишинга и фишинга;**
- **Завладение денежными средствами путем обмана с использованием сети Интернет (социальных сетей);**
- **Несанкционированный доступ к учетным записям в социальных сетях, мессенджерах, электронной почты, онлайн-играх;**
- **Блокировка с использованием вирусов ПЭВМ, Интернет – браузера, информации с требованием дальнейшей оплаты за разблокировку.**

Вишинг

Вишинг – форма мошенничества, основанная на социальной инженерии. Злоумышленники, используя телефон либо мессенджеры в сети Интернет и играя определенную роль (сотрудников банков, правоохранительных органов), под различными предлогами путем обмана пытаются получить личную и финансовую информацию клиентов банков либо склонить их к совершению определенных действий с целью дальнейшего хищения денежных средств.

Вишинг

Предлоги для передачи данных:

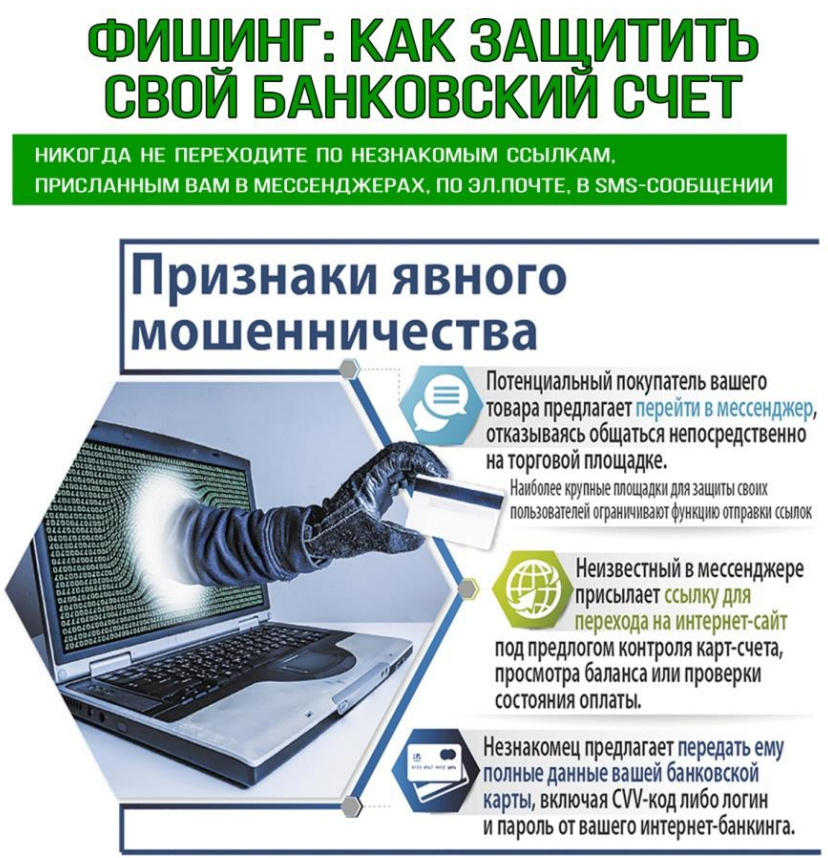
- **«Осуществление по Вашей карте мошеннической операции и необходимость срочной ее отмены»;**
- **«Оформление на Ваше имя онлайн-кредита и принятие срочных мер по его отклонению».**

Злоумышленников интересует:

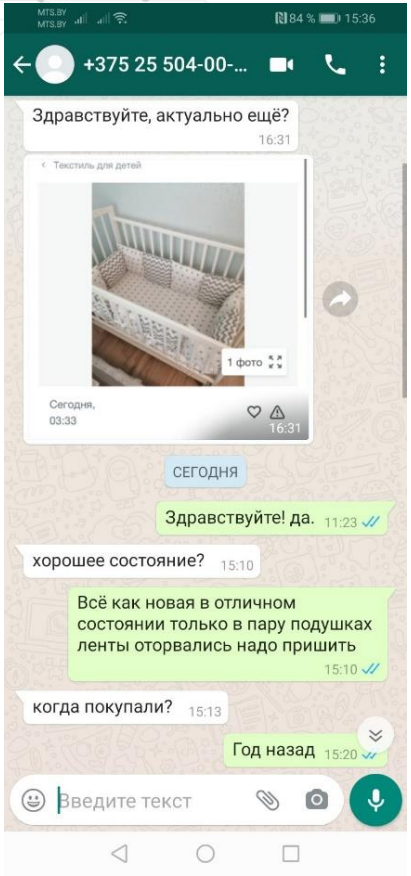
- **Идентификационный номер и иные паспортные данные клиента;**
- **Номер карты, срок действия, имя владельца и CVV/CVC-код;**
- **Коды подтверждения, приходящие на Ваш номер телефона sms либо puch уведомлениями;**
- **Реквизиты доступа к системе Интернет-банк: логин, пароль, сеансовый ключ).**

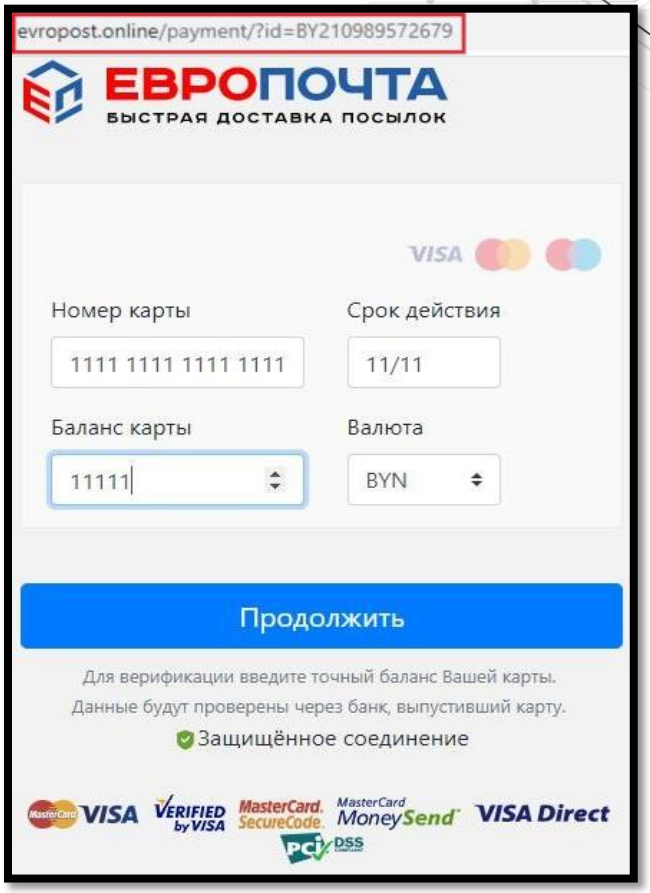
Фишинг

Фишинг – злоумышленники в ходе переписки в социальных сетях, на торговых Интернет-площадках объявлений под различными предлогами (оплата за товар, за доставку почтовой службе), пытаются склонить пользователя к переходу в сети по указанной ими ссылке. В результате пользователь переходит на фальшивый ресурс и вводит на нем свои персональные данные (реквизиты доступа к Интернет–банкингу, банковских платежных карточек), с помощью которых злоумышленники и похищают денежные средства граждан.

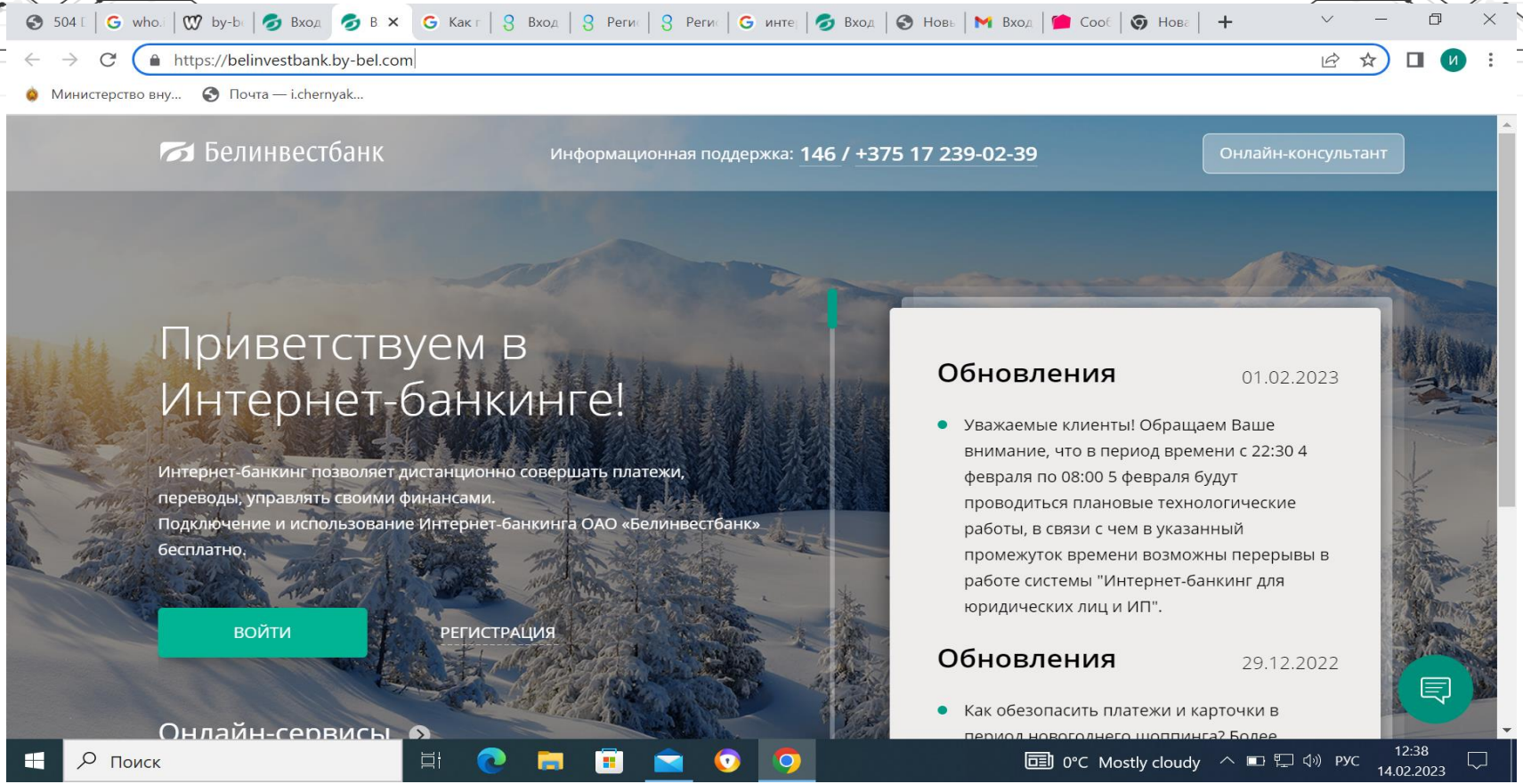


Пример фишинга





Пример фишинга

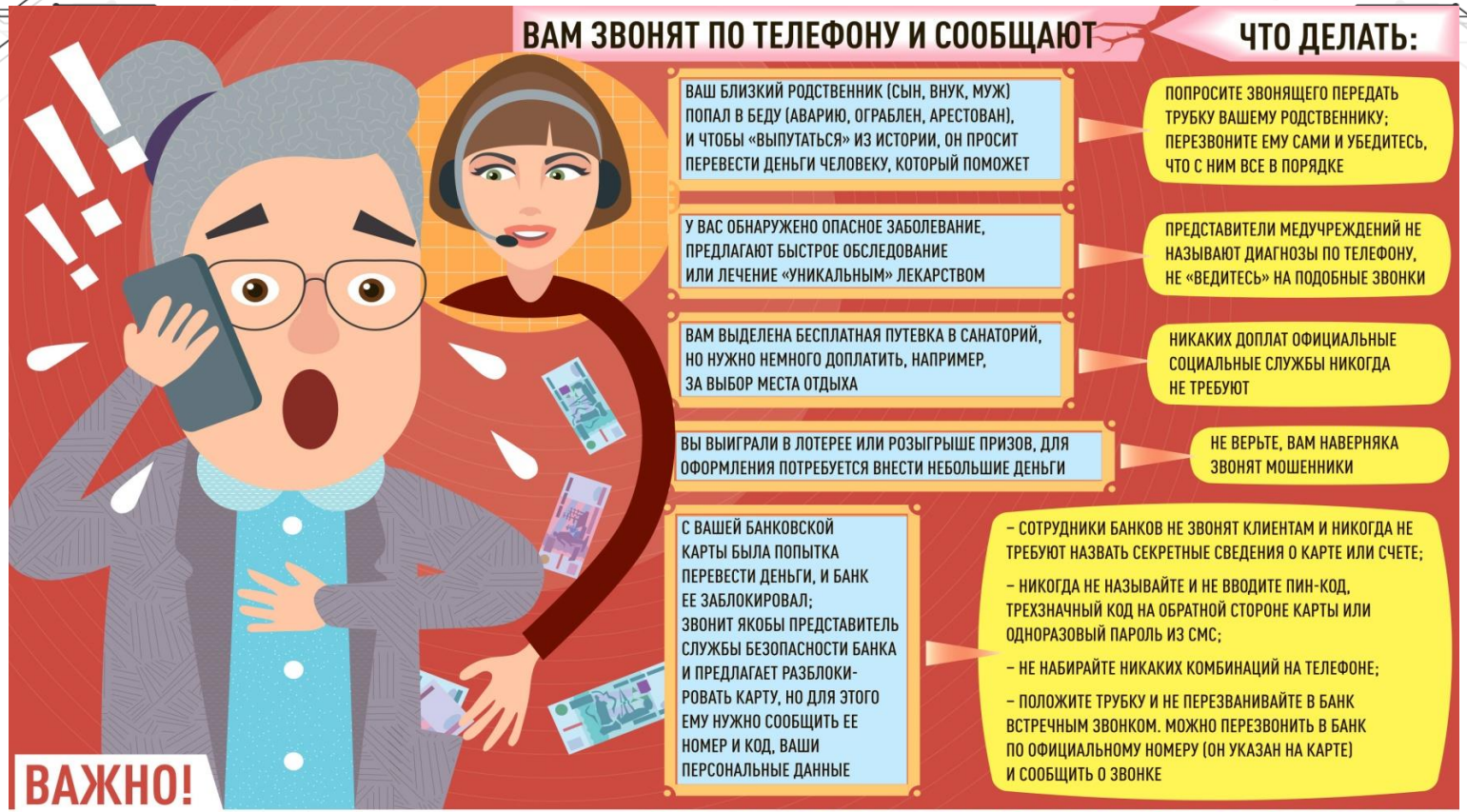


Мошенничество

Наиболее распространенные способы хищений денежных средств:

- **Перечисление денег в долг и под проценты;**
- **Под видом валютно–обменных операций, в том числе с использованием криптовалюты и электронных – платежных систем;**
- **Вложение денежных средств с целью осуществления трейдинговой, брокерской и т.д. деятельностью, участие в финансовых пирамидах;**
- **Под видом получения призов, наследства, выигрыша в лотереи и т.д.;**
- **Фальшивые объявления о трудоустройстве на работу;**
- **«Брачные» аферисты (входят в доверие к женщинам с целью получения под различными предлогами денежных средств);**
- **Сбор благотворительных пожертвований.**

Мошенничество



Несанкционированный доступ

Несанкционированный доступ к учетным записям («взлом») осуществляется из определенной заинтересованности:

- **Личной – желание ознакомиться с информацией в анкете, изменить, удалить либо скопировать её, а также для удовлетворения своих способностей и навыков «взлома» с целью самоутверждения;**
- **Корыстной – осуществление доступа за вознаграждение либо, в большинстве случаев – для подготовки и совершения других корыстных преступлений (хищений).**

Атаки на предприятия и организации

Основные схемы:

- **Шифрование коммерческой информации;**
- **Подмена реквизитов для перевода средств;**
- **Шифрование с использованием фишинговых писем;**

Правила «цифровой» гигиены

Правила «цифровой» гигиены

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

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 пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ 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

× 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 03

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

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

6 правил информационной безопасности

главное управление по противодействию киберпреступности КМ МВД Беларуси

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

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 и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ 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

× Размещать персональную и контактную информацию о себе в открытом доступе
× Использовать указание геолокации 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 отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ 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 CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

× 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.

Правила «цифровой» гигиены

- **Использовать сложные пароли и периодически их менять;**
- **Не сохранять пароли в браузерах, не хранить их на бумажных носителях в доступных местах;**
- **Использовать антивирусное программное обеспечение;**
- **Устанавливать приложения только из проверенных источников;**
- **Не переходить по подозрительным ссылкам, не открывать подозрительные письма и вложения к ним;**
- **Не использовать для переписки e-mail, к которому привязаны устройства, учетные записи, Интернет-банкинг;**
- **Обмениваться сообщениями в мессенджерах только полностью удостоверившись в личности собеседника.**

Правила «цифровой» гигиены

- **Внимательно ознакомиться с правилами использования банковскими платежными карточками Вашего банка;**
- **Не передавать карту, ее реквизиты, иную личную и финансовую информацию третьим лицам;**
- **Использовать отдельную карту для Интернет-покупок и не хранить на ней деньги;**
- **Подключить услуги 3D-Secure, SMS-информирование, установить необходимые лимиты;**
- **Осуществлять оплату в сети Интернет** 

енных ресурсах, работающих по безопасному протоколу ;
- **Проявлять внимание и бдительность.**

Спасибо за внимание!

Матяс Артем Геннадьевич

Начальник УПК КМ
УВД Гродненского облисполкома