

Актуальные способы совершения киберпреступлений. Безопасность в сети Интернет.

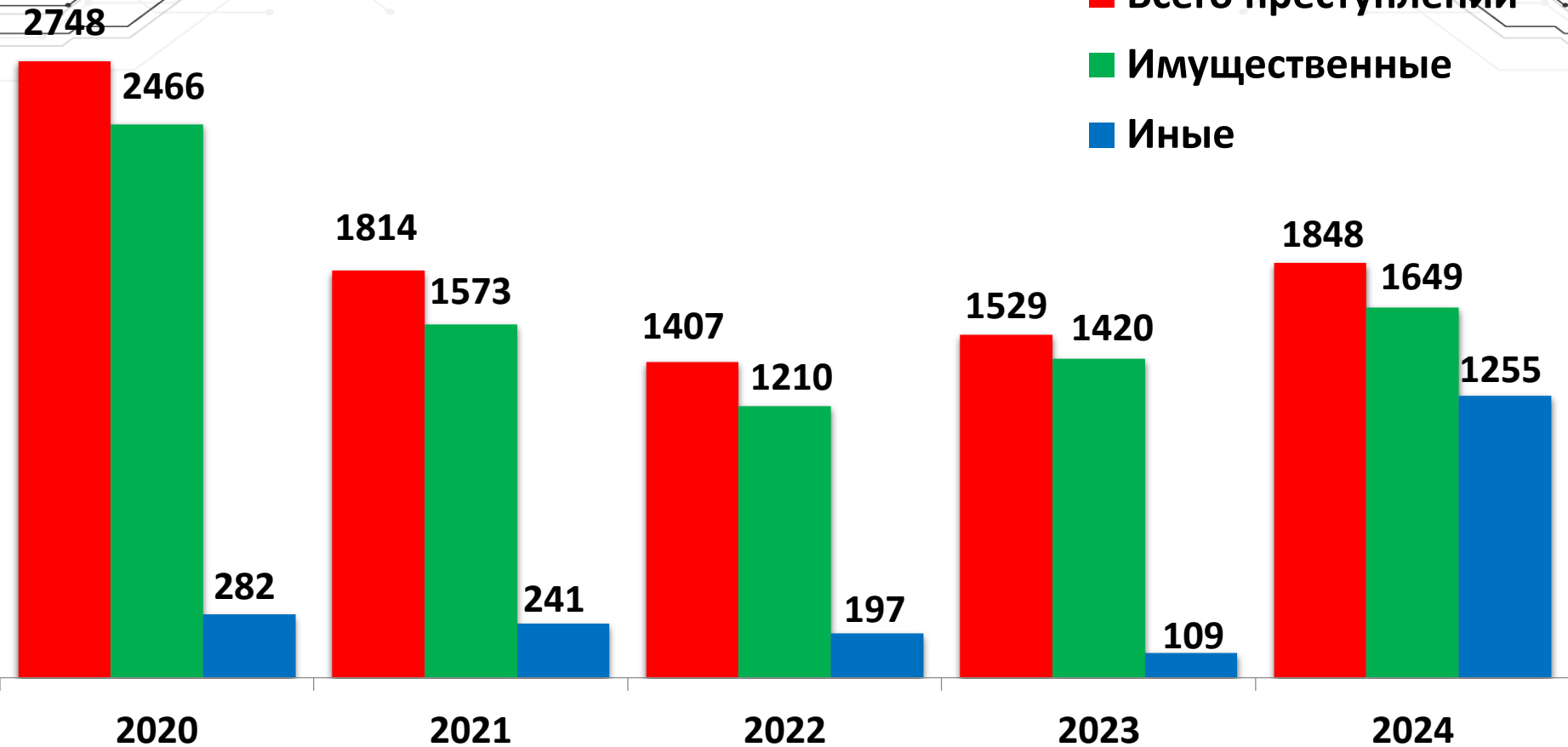


Матяс Артем Геннадьевич

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 предложениями путем обмана пытаются получить личную и финансовую информацию клиентов банков либо склонить их к совершению определенных действий с целью дальнейшего хищения денежных средств.

ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ



НЕ следуй инструкциям
незнакомцев, позвонившим
с неизвестного номера



НЕ сообщай неизвестным
лицам свои персональные
данные



НЕ совершай никаких
действий на смартфоне по
просьбе посторонних лиц



НЕ переводи деньги
незнакомым людям в
качестве предоплаты



Сохрани эту информацию и поделись с другими



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 push 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 предложениями (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.

ФИШИНГ: КАК ЗАЩИТИТЬ СВОЙ БАНКОВСКИЙ СЧЕТ

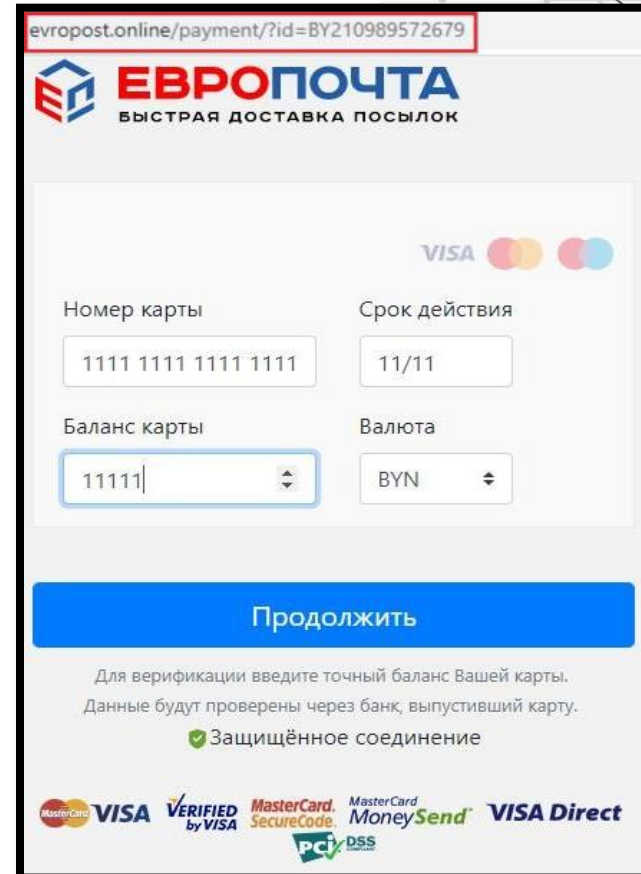
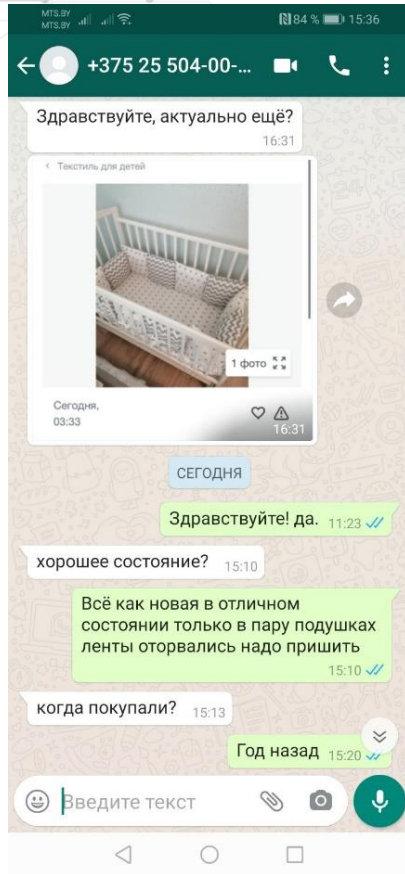
НИКОГДА НЕ ПЕРЕХОДИТЕ ПО НЕЗНАКОМЫМ ССЫЛКАМ, ПРИСЛАННЫМ ВАМ В МЕССЕНДЖЕРАХ, ПО ЭЛ.ПОЧТЕ, В SMS-СООБЩЕНИИ

Признаки явного мошенничества



-  Потенциальный покупатель вашего товара предлагает перейти в мессенджер, отказываясь общаться непосредственно на торговой площадке.
Наиболее крупные площадки для защиты своих пользователей ограничивают функцию отправки ссылок
-  Неизвестный в мессенджере присылает ссылку для перехода на интернет-сайт под предлогом контроля карт-счета, просмотра баланса или проверки состояния оплаты.
-  Незнакомец предлагает передать ему полные данные вашей банковской карты, включая CVV-код либо логин и пароль от вашего интернет-банкинга.

Пример фишинга



Пример фишинга

504 | who | W by-bi | Вход | В x | Как г | Вход | Реги | Реги | инте | Вход | Новь | Вход | Соот | Новь | +

← → ↻ | <https://belinvestbank.by-bel.com> | 🏠 ☆ 🗄️ И ⋮

Министерство вну... | Почта — i.chernyak...

Белинвестбанк | Информационная поддержка: 146 / +375 17 239-02-39 | [Онлайн-консультант](#)

Приветствуем в Интернет-банкинге!

Интернет-банкинг позволяет дистанционно совершать платежи, переводы, управлять своими финансами.
Подключение и использование Интернет-банкинга ОАО «Белинвестбанк» бесплатно.

[ВОЙТИ](#) | [РЕГИСТРАЦИЯ](#)

Онлайн-сервисы

Обновления

01.02.2023

- Уважаемые клиенты! Обращаем Ваше внимание, что в период времени с 22:30 4 февраля по 08:00 5 февраля будут проводиться плановые технологические работы, в связи с чем в указанный промежуток времени возможны перерывы в работе системы "Интернет-банкинг для юридических лиц и ИП".

Обновления

29.12.2022

- Как обезопасить платежи и карточки в период новогоднего шоппинга? Более

0°C Mostly cloudy | 12:38 14.02.2023

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 предложениями денежных средств);**
- **Сбор благотворительных пожертвований.**

Мошенничество

ВАМ ЗВОНЯТ ПО ТЕЛЕФОНУ И СООБЩАЮТ

ЧТО ДЕЛАТЬ:

ВАШ БЛИЗКИЙ РОДСТВЕННИК (СЫН, ВНУК, МУЖ) ПОПАЛ В БЕДУ (АВАРИЮ, ОГРАБЛЕН, АРЕСТОВАН), И ЧТОБЫ «ВЫПУТАТЬСЯ» ИЗ ИСТОРИИ, ОН ПРОСИТ ПЕРЕВЕСТИ ДЕНЬГИ ЧЕЛОВЕКУ, КОТОРЫЙ ПОМОЖЕТ

ПОПРОСИТЕ ЗВОНЯЩЕГО ПЕРЕДАТЬ ТРУБКУ ВАШЕМУ РОДСТВЕННИКУ; ПЕРЕЗВОНИТЕ ЕМУ САМИ И УБЕДИТЕСЬ, ЧТО С НИМ ВСЕ В ПОРЯДКЕ

У ВАС ОБНАРУЖЕНО ОПАСНОЕ ЗАБОЛЕВАНИЕ, ПРЕДЛАГАЮТ БЫСТРОЕ ОБСЛЕДОВАНИЕ ИЛИ ЛЕЧЕНИЕ «УНИКАЛЬНЫМ» ЛЕКАРСТВОМ

ПРЕДСТАВИТЕЛИ МЕДУЧРЕЖДЕНИЙ НЕ НАЗЫВАЮТ ДИАГНОЗЫ ПО ТЕЛЕФОНУ, НЕ «ВЕДИТЕСЬ» НА ПОДОБНЫЕ ЗВОНКИ

ВАМ ВЫДЕЛЕНА БЕСПЛАТНАЯ ПУТЕВКА В САНАТОРИЙ, НО НУЖНО НЕМНОГО ДОПЛАТИТЬ, НАПРИМЕР, ЗА ВЫБОР МЕСТА ОТДЫХА

НИКАКИХ ДОПЛАТ ОФИЦИАЛЬНЫЕ СОЦИАЛЬНЫЕ СЛУЖБЫ НИКОГДА НЕ ТРЕБУЮТ

ВЫ ВЫИГРАЛИ В ЛОТЕРЕЕ ИЛИ РОЗЫГРЫШЕ ПРИЗОВ, ДЛЯ ОФОРМЛЕНИЯ ПОТРЕБУЕТСЯ ВНЕСТИ НЕБОЛЬШИЕ ДЕНЬГИ

НЕ ВЕРЬТЕ, ВАМ НАВЕРНЯКА ЗВОНЯТ МОШЕННИКИ

С ВАШЕЙ БАНКОВСКОЙ КАРТЫ БЫЛА ПОПЫТКА ПЕРЕВЕСТИ ДЕНЬГИ, И БАНК ЕЕ ЗАБЛОКИРОВАЛ; ЗВОНИТ ЯКОБЫ ПРЕДСТАВИТЕЛЬ СЛУЖБЫ БЕЗОПАСНОСТИ БАНКА И ПРЕДЛАГАЕТ РАЗБЛОКИРОВАТЬ КАРТУ, НО ДЛЯ ЭТОГО ЕМУ НУЖНО СООБЩИТЬ ЕЕ НОМЕР И КОД, ВАШИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

– СОТРУДНИКИ БАНКОВ НЕ ЗВОНЯТ КЛИЕНТАМ И НИКОГДА НЕ ТРЕБУЮТ НАЗВАТЬ СЕКРЕТНЫЕ СВЕДЕНИЯ О КАРТЕ ИЛИ СЧЕТЕ;
– НИКОГДА НЕ НАЗЫВАЙТЕ И НЕ ВВОДИТЕ ПИН-КОД, ТРЕХЗНАЧНЫЙ КОД НА ОБРАТНОЙ СТОРОНЕ КАРТЫ ИЛИ ОДНОРАЗОВЫЙ ПАРОЛЬ ИЗ СМС;
– НЕ НАБИРАЙТЕ НИКАКИХ КОМБИНАЦИЙ НА ТЕЛЕФОНЕ;
– ПОЛОЖИТЕ ТРУБКУ И НЕ ПЕРЕЗВАНИВАЙТЕ В БАНК ВСТРЕЧНЫМ ЗВОНКОМ. МОЖНО ПЕРЕЗВОНИТЬ В БАНК ПО ОФИЦИАЛЬНОМУ НОМЕРУ (ОН УКАЗАН НА КАРТЕ) И СООБЩИТЬ О ЗВОНКЕ

ВАЖНО!

МОШЕННИКИ ВОРУЮТ БАЗЫ ДАННЫХ И НАЗЫВАЮТ ВАС ПО ИМЕНИ-ОТЧЕСТВУ, А В ТЕЛЕФОНЕ ВИДЕН НОМЕР ВАШЕГО БАНКА

БУДЬТЕ ГОТОВЫ И ПРОЯВИТЕ БДИТЕЛЬНОСТЬ

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;

ВНИМАНИЕ!
АТАКА НА ГОСОРГАНИЗАЦИИ!

СПЕЦИАЛИСТЫ ОТМЕЧАЮТ УВЕЛИЧЕНИЕ ЧИСЛА ФИШИНГОВЫХ АТАК НА ЭЛЕКТРОННЫЕ ПОЧТОВЫЕ ЯЩИКИ ГОСОРГАНИЗАЦИЙ!

ПРИ РАБОТЕ С ЭЛЕКТРОННОЙ ПОЧТОЙ

НЕ НАДО:	НАДО:
ОТКРЫВАТЬ ВЛОЖЕНИЯ ПОЧТОВЫХ СООБЩЕНИЙ ОТ НЕИЗВЕСТНЫХ ОТПРАВИТЕЛЕЙ	ПОДКЛЮЧИТЬ 2-ФАКТОРНУЮ АУТЕНТИФИКАЦИЮ
ПЕРЕХОДИТЬ ПО ССЫЛКАМ, ПОЛУЧЕННЫМ ОТ НЕИЗВЕСТНЫХ	РЕГУЛЯРНО МЕНЯТЬ ПАРОЛЬ ЭЛ.ПОЧТЫ
ХРАНИТЬ И ПЕРЕДАВАТЬ В ОТКРЫТОМ ВИДЕ ВАЖНЫЕ ДАННЫЕ (ЗААРХИВИРУЙТЕ ИХ И УСТАНОВИТЕ ПАРОЛЬ)	ИСПОЛЬЗОВАТЬ НЕКОЛЬКО ПОЧТОВЫХ ЯЩИКОВ ДЛЯ РАЗНЫХ РЕСУРСОВ (ПЕРЕПИСКА, РЕГИСТРАЦИЯ, ДЕЛОВАЯ ПОЧТА)
ПРИ РЕГИСТРАЦИИ ЯЩИКА УКАЗЫВАТЬ БИОГРАФИЧЕСКИЕ ДАННЫЕ. ИСПОЛЬЗОВАТЬ ПРОСТЫЕ ПАРОЛИ И ПОВТОРЯЮЩИЕСЯ СИМВОЛЫ	ИСПОЛЬЗОВАТЬ УНИКАЛЬНЫЕ ПАРОЛИ ДЛЯ РАЗНЫХ ИНТЕРНЕТ-РЕСУРСОВ
	ВВОДИТЬ ИНФОРМАЦИЮ ТОЛЬКО НА ЗАЩИЩЕННЫХ САЙТАХ (HTTPS)

ВНИМАНИЕ!
ЕДИНСТВЕННЫЙ НАДЕЖНЫЙ СПОСОБ ЗАЩИТЫ
- ЭТО ВАША БДИТЕЛЬНОСТЬ!

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ КМ МВД БЕЛАРУСИ

Правила «цифровой» гигиены

ГЛАВНЫЕ ПРАВИЛА **ЦИФРОВОЙ ГИГИЕНЫ** ДЛЯ ДЕТЕЙ

Не сообщай личную информацию незнакомцу. И, вообще, в интернете не размещай сведения о себе и семье

Советуйся с родителями, как правильно поступить, если столкнулся с чем-то непонятным или пугающим

Помни, что в интернете надо быть очень-очень внимательным. Старайся избегать общения с незнакомыми людьми в онлайн-играх и соцсетях, не выполняй бездумно то, что они попросят тебя сделать

ГЛАВНОЕ УПРАВЛЕНИЕ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ МВД



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  <https://> енных ресурсах, работающих по безопасному протоколу ;**
- **Проявлять внимание и бдительность.**

Спасибо за внимание!



Матяс Артем Геннадзьевич

Начальник УПК КМ

УВД Гродненского облисполкома