Профилактика киберпреступлений

Сеть Интернет стала практически незаменимым средством повседневной связи и обмена информацией по всему миру, и преступники не могут этим не пользоваться. Два миллиарда пользователей Интернета по всему миру создают идеальную среду для совершения преступлений, где можно действовать анонимно и получать доступ к любой персональной информации, которую мы, желая того или нет, размещаем в сети. В последние годы безопасность в сети Интернет подвергается более серьезным угрозам, и от преступлений в глобальном киберпространстве страдают более 431 миллиона взрослых пользователей.

Правила информационной безопасности:

1. **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 бумажном носителе; использовать в качестве пароля свой логин; сохранять пароли автоматически в браузере; использовать биографическую информацию в пароле.

2. **БЕЗОПАСНЫЙ Wi-Fi**

НЕОБХОДИМО: отключить общий доступ к своей Wi-Fi точке, даже если у вас "безлимитный" интернет; использовать надежный 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.

3. **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 (нет https)

4. **БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ**

НЕОБХОДИМО: подключать 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 неизвестных отправителей: скорее всего это спам или мошенники; открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл.

5. **ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ 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 соцсетях - лучше напишите об этом администратору ресурса; употреблять ненормативную лексику при общении.

6. **ЗАЩИТА БАНКОВСКИХ КАРТОЧЕК**

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 максимальную сумму 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» доступа к системе «Интернет – банкинг»; сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароли 3-D Secure.

Профилактические листовки **здесь**

Профилактические видеоролики кибермошеничества и преступлений **здесь**

Если Вы стали жертвой киберпреступников, обращайтесь в главное управление по противодействию киберпреступности криминальной милиции МВД Беларуси

Кибербезопасность https://www.mvd.gov.by/ru/news/7021

Профилактика киберпреступлений
https://drive.google.com/drive/folders/1xoteXMBwfpQFqzfO6tK1EBdTLwSvNCVh

Информация по профилактике киберпреступлений
Видеоролик по кибербезопасности
#Простые правила: делаем интернет безопасным вместе
Безопасность в интернете
Вишинг
ЗВУК 2021
Осторожно ВИШИНГ
Как не стать жертвой киберпреступника


КИБЕР-
ВИКТОРИНА!
ПРОЙДИ ТЕСТ
Больше информации
в Telegram-канале
Цифровая грамотность
t.me/cifgram
ПОДПИШИСЬ НА КАНАЛ


БЫТЬ ХАКЕРОМ -
БОЛЬШЕ ИНФОРМАЦИИ
В TELEGRAM-КАНАЛЕ
ЦИФРОВАЯ ГРАМОТНОСТЬ
T.ME/CIFGRAM
УПРАВЛЕНИЕ
ПО ПРОТИВОДЕЙСТВИЮ
КИБЕРПРЕСТУПНОСТИ
УВД ВИТЕБСКОГО
ОБЛИСПОЛКОМА
НЕ РАЗВЛЕЧЕНИЕ,
А ПРЕСТУПЛЕНИЕ
УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ
ЗА КИБЕРПРЕСТУПЛЕНИЯ НАСТУПАЕТ:
с 14 лет
статья 212 УК
Хищение имущества путем модификации компьютерной информации
наказывается вплоть до лишения свободы на срок до 12 лет
статья 340 УК
Заведомо ложное сообщение об опасности
наказывается вплоть до лишения свободы на срок до 7 лет
с 16 лет
статья 222 УК
Незаконный оборот средств платежа и (или) инструментов
наказывается вплоть до лишения свободы на срок до 10 лет
статья 349 УК
Несанкционированный доступ к компьютерной информации
наказывается вплоть до лишения свободы на срок до 7 лет

СТАТЬЯ 212
Уголовного Кодекса Республики Беларусь

Хищение путем использования компьютерной техники

Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации наказывается лишением свободы на срок

ДО ТРЕХ ЛЕТ.

МИЛИЦИЯ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ МВД РБ

ОСТОРОЖНО! МОШЕННИКИ!

Телефонные мошенники представляются сотрудниками правоохранительных органов или банка. Под различными предлогами убеждают участвовать в «спецоперации по разоблачению мошенников». Для этого уговаривают оформить кредиты и перевести деньги на «специальный защищенный счет».

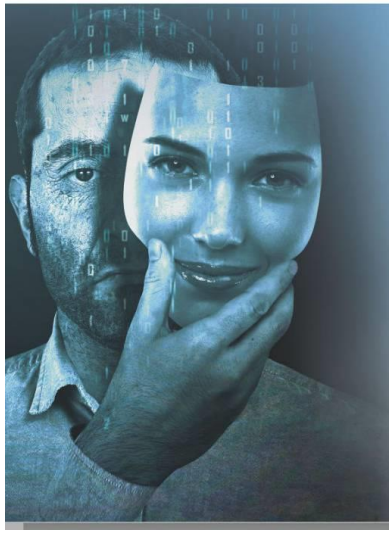
ПО ПРОСЬБЕ НЕЗНАКОМЫХ ЛИЦ:

- **НЕ сообщайте данные карты и коды из СМС-сообщений от банка, логины и пароли доступа к сервисам**
- **НЕ устанавливайте программы не передавайте коды регистрации**
- **НЕ оформляйте кредиты**
- **НЕ переводите деньги на «защищенный счет»**

Больше информации в Telegram-канале Цифровая грамотность t.me/cifgram

Если вам поступил звонок из «банка», завершите разговор и перезвоните в банк

Установите в Viber защиту от лишних звонков



БУДЬТЕ БДИТЕЛЬНЫ!

НЕ СТАНЬТЕ ЖЕРТВОЙ ОБМАНА!

Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома


ТЕЛЕФОННЫЕ МОШЕННИКИ
МОГУТ ПРЕДСТАВИТЬСЯ РАБОТНИКАМИ БАНКА или ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ
НЕ сообщайте данные карты и коды из СМС
НЕ оформляйте кредиты по просьбе третьих лиц
НЕ устанавливайте программы по просьбе третьих лиц
НЕ переводите деньги на «защищенный счет»
НЕ переходите по ссылкам от незнакомцев
Больше информации в Telegram-канале Цифровая грамотность t.me/clfgram
ПЕРЕЗВОНИТЕ В БАНК!
если предлагают отменить расходную операцию, которую вы не совершали
если убеждают установить программу на ваше устройство
если убеждают оформить кредит и перевести деньги на «защищенный» счет
если просят назвать данные для отмены якобы оформленной доверенности на операции по вашему вкладу
если вам одобрен кредит, который вы не оформляли
ПЕРЕЗВОНИТЕ В МИЛИЦИЮ!
если просят поучаствовать в «разоблачении недобросовестного сотрудника банка»
УСТАНОВИТЕ В VIBER ЗАЩИТУ ОТ ЛИШНИХ ЗВОНКОВ
Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома


ОСТОРОЖНО! МОШЕННИКИ В ИНТЕРНЕТЕ
https:// оплата .by/
https:// банк
https:// доставка
ПОЛЬЗУЙСЯ БЕЗОПАСНО
Пользуйтесь мобильными приложениями банка
Переходите в интернет-банкинг только с официального сайта банка
Проверяйте адрес интернет-банкинга в адресной строке, между последней точкой и первой наклонной чертой должно быть только так .by/
Активируйте на карте, используемой для онлайн-платежей, услугу 3-D Secure (подтверждение платежей SMS-кодом)
Не переходите в интернет-банкинг по ссылкам в поисковых системах
Не используйте SMS-коды от банка и код с оборотной стороны карты для получения денежных средств
Управление по противодействию киберпреступности криминальной милиции УВД Витебского облисполкома

НАУЧИТЕ СВОИХ РОДИТЕЛЕЙ ФИНАНСОВОЙ ГРАМОТНОСТИ

ПО ПРОСЬБЕ ТРЕТЬИХ ЛИЦ

НЕ УСТАНАВЛИВАЙТЕ ПРОГРАММЫ

НЕ ПЕРЕВОДИТЕ ДЕНЬГИ

Управление по противодействию киберпреступности
криминальной милиции УВД Витебского облисполкома