



Основные аспекты профилактики киберпреступности

*Матуйзо Андрей,
депутат Молодёжного парламента
«Юность» Вороновского района*





**МОЛОДЁЖНЫЙ
ПАРЛАМЕНТ
ВОРОНОВСКИЙ РАЙОН**

«ЮНОСТЬ»

Киберпреступность —

это

**любая преступная
активность в
виртуальном
пространстве.**

Примеры рассылки в соцсетях

– «Привет, у тебя есть действующая банковская карточка? Мою заблокировали, а как раз сегодня мне должны перечислить деньги. Можно я дам реквизиты твоей карты, на нее придут деньги, потом переведешь мне, когда мою карту разблокируют. В долгу не останусь!»;

– «Какого банка у тебя карточка? Мне нужна VISA или MasterCard для оплаты в интернете. Можешь дать реквизиты или сфотографировать? Там еще на обратной стороне три цифры есть. Тебе на телефон должен придти код, напиши сюда. Нет, не беспокойся, я деньги верну с комиссией.»;

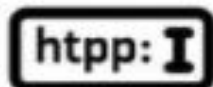
– «Можешь дать логин и пароль от интернет-банкинга. В моем выдает какую-то ошибку, хочу проверить, есть ли в твоём такой баг. Платежей делать не буду, мы же друзья!»

ОСТОРОЖНО!

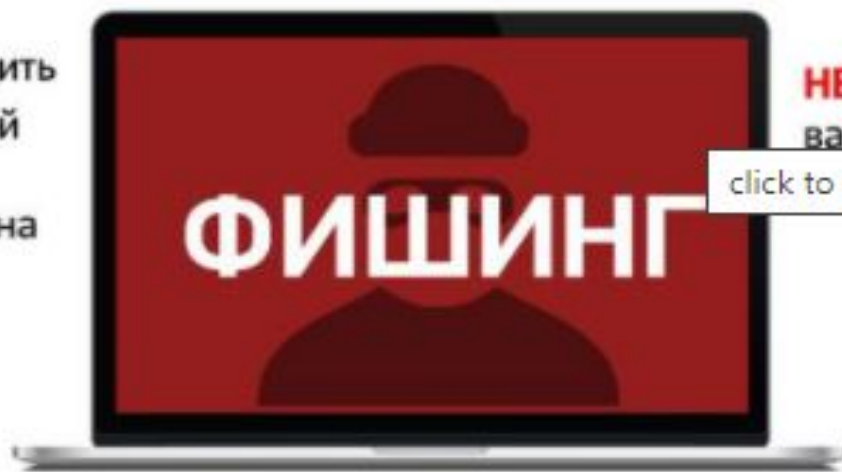
МОШЕННИКИ В ИНТЕРНЕТЕ



Не торопись переходить по ссылке, полученной от незнакомца: возможно, она ведет на фишинговый сайт



Не спеши переходить по ссылке: введи адрес вручную



НЕ пользуйся открытыми вай-фай-сетями в кафе и на улице



Фишинговая ссылка может прийти в мессенджере, по электронной почте, в смс-сообщении

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

ВНИМАНИЕ!

ЗАЩИТИ СВОЮ БАНКОВСКУЮ КАРТУ



Хранить пинкод вместе
с картой



Распространять
личные данные, логин
и пароль доступа к
системе
«Интернет-банкинг»

НЕЛЬЗЯ



click to close

НЕЛЬЗЯ CVV-код или
отправлять его фото



Сообщать данные,
полученные в виде
SMS-сообщений,
сеансовые пароли, код
авторизации и т.д.

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

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

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 )

- + 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.

Спасибо за внимание!

Маленькие шаги оставляют большие следы!