СОВЕТЫ ПО ЗАЩИТЕ ОТ КИБЕРПРЕСТУПНИКОВ

**Понимание того, что такое киберпреступение, какие типы киберпреступлений существуют и как от них защититься, поможет вам чувствовать себя увереннее.**

**Что такое киберпреступление**

Киберпреступление – это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство (но не все) киберпреступления совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями.

Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

Киберпреступники редко взламывают компьютеры по причинам, не имеющим отношения к получению прибыли, например, по политическим или личным.

**Типы киберпреступлений**

Вот несколько примеров различных типов киберпреступлений:

* Мошенничество с электронной почтой и интернет-мошенничество
* Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
* Кража финансовых данных или данных банковских карт
* Кража и продажа корпоративных данных
* Кибершантаж (требование денег для предотвращения кибератаки)
* Атаки программ-вымогателей (тип кибершантажа)
* Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
* Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)
* Большинство киберпреступлений относится к одной из двух категорий
* Криминальная деятельность, целью которой являются сами компьютеры
* Криминальная деятельность, в которой компьютеры используются для совершения других преступлений

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью зловредов можно удалять или похищать данные.

Киберпреступления, в результате которых владельцы устройств не могут пользоваться своими компьютерами или сетью, а компании – предоставлять интернет-услуги своим клиентам, называется атакой отказа в обслуживании (DoS).

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений.

Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры с вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети.

Киберпреступники могут также выполнять так называемую атаку с распределенным отказом в обслуживании (DDos). Она похожа на DoS-атаку, но для ее проведения преступники используют множество скомпрометированных компьютеров.

Также, еще есть третья категория киберпреступлений, когда компьютер используется как соучастник незаконного деяния, например, для хранения на нем украденных данных.

**Примеры киберпреступлений**

* **Атаки с использованием вредоносного ПО**

Атака с использованием вредоносного ПО – это заражение компьютерной системы или сети компьютерным вирусом или другим типом вредоносного ПО.

Компьютер, зараженный вредоносной программой, может использоваться злоумышленниками для достижения разных целей. К ним относятся кража конфиденциальных данных, использование компьютера для совершения других преступных действий или нанесение ущерба данным.

* **Фишинг**

Фишинговая кампания – это массовая рассылка спам-сообщений или других форм коммуникации с целью заставить получателей выполнить действия, которые ставят под угрозу их личную безопасность или безопасность организации, в которой они работают.

Сообщения в фишинговой рассылке могут содержать зараженные вложения или ссылки на вредоносные сайты. Они также могут просить получателя в ответном письме предоставить конфиденциальную информацию.

Другой тип фишинговой кампании известен как целевой фишинг.

Мошенники пытаются обмануть конкретных людей, ставя под угрозу безопасность организации, в которой они работают.

В отличие от массовых неперсонифицированных фишинговых рассылок сообщения для целевого фишинга создаются так, чтобы у получателя не возникло сомнений, что они отправлены из надежного источника, например, от генерального директора или IT-менеджера.

* **Распределённые атаки типа «отказ в обслуживании»**

Распределенные типа «отказ в обслуживании» (DDoS) – это тип кибератаки, которую злоумышленники используют для взлома системы или сети. Иногда для запуска DDoS-атак используются подключенные устройства IoT (Интернет вещей).

DDoS-атака перегружает систему большим количеством запросов на подключение, которые она рассылает через один из стандартных протоколов связи.

Кибершантажисты могут использовать угрозу DDoS-атаки для получения денег. Кроме того, DDoS запускают в качестве отвлекающего маневра в момент совершения другого типа киберпреступления.

**Как не стать жертвой киберпреступления**

Итак, теперь, когда вы понимаете, какую угрозу представляет киберпреступность, встает вопрос о том, как наилучшим образом защитить ваш компьютер и личные данные? Следуйте следующим советам:

* **Регулярно обновляйте ПО и операционную систему**

Постоянное обновление программного обеспечения и операционной системы гарантирует, что для защиты вашего компьютера используются новейшие исправления безопасности.

* **Установите антивирусное ПО и регулярно его обновляйте**

Использование антивируса или комплексного решения для обеспечения интернет-безопасности. Антивирусное ПО позволяет проверять, обнаруживать и удалять угрозы до того, как они создадут проблему. Оно помогает защитить ваш компьютер и ваши данные от киберпреступников.

Если вы используете антивирусное программное обеспечение, регулярно обновляйте его, чтобы обеспечить наилучший уровень защиты.

* **Используйте сложные пароли**

Используйте сложные пароли, которые трудно подобрать, и нигде их не записывайте. Можно воспользоваться услугой надежного менеджера паролей, который облегчит вам задачу, предложив сгенерированный им сильный пароль.

* **Не открывайте вложения в электронных спам-сообщениях**

Классический способ заражения компьютеров с помощью вредоносных атак и других типов киберпреступлений - это вложения в электронных спам-сообщениях. Никогда не открывайте вложение от неизвестного вам отправителя.

* **Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете**

Еще один способ, используемый киберпреступниками для заражения компьютеров пользователей, - это вредоносные ссылки в спамовых электронных письмах или других сообщения, а также на незнакомых веб-сайтах. Не проходите по этим ссылкам, чтобы не стать жертвой интернет-мошенников.

* **Не предоставляйте личную информацию, не убедившись в безопасности канала передачи**

Никогда не передавайте личные данные по телефону или по электронной почте, если вы не уверены, что телефонное соединение или электронная почта защищены. Убедитесь, что вы действительно говорите именно с тем человеком, который вам нужен.

* **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос**

Если звонящий просит вас предоставить какие-либо данные, положите трубку. Перезвоните в компанию напрямую по номеру телефона на ее официальном сайте, и убедитесь, что вам звонили не мошенники.

Желательно пользоваться, при этом, другим телефоном, потому что злоумышленники могут оставаться на линии: вы будете думать, что набрали номер заново, а они будут отвечать якобы от имени банка или другой организации, с которой, по вашему мнению, вы разговариваете.

* **Внимательно проверяйте адреса веб-сайтов, которые вы посещаете**

Обращайте внимание на URL-адреса сайтов, на которые вы хотите зайти. Они выглядят легитимно? Не переходить по ссылкам, содержащим незнакомые или на вид спамовые URL-адреса.

Если ваш продукт (банковская платежная карта) для обеспечения безопасности в Интернете включает функцию защиты онлайн-транзакций, убедитесь, что она активирована.

* **Внимательно просматривайте свои банковские выписки и**запрашивайте в банке информацию по любым незнакомым транзакциям. Банк может проверить, являются ли они мошенническими.

<https://mir.pravo.by/edu/internet-i-rebenok/sovety-po-zashchite-ot-kiberprestupnikov/>

# Киберликбез

#### Фишинг

Это поддельные сообщения-ссылки вроде «Вам поступил денежный перевод», которые приходят на электронную почту (чаще), через СМС или мессенджеры.

Если просто откроете (прочтете) сообщение - ничего страшного. Но как только перейдете по зараженной ссылке внутри письма или введете там персональную информацию - мошенники получат доступ к данным на компьютере или телефоне. Им не составит труда захватить ваши странички в соцсетях, украсть реквизиты банковских карт.

ПЕРЕХОДИТЬ ПО ССЫЛКАМ ИЗ ПОДОЗРИТЕЛЬНЫХ платежных ПИСЕМ НЕЛЬЗЯ

#### Вишинг

Это прием, когда мошенники выведывают логины/пароли через звонок по телефону. Узнав нужные данные, преступники снимают с карты деньги и исчезают навсегда.

Если посторонний просит CVV-код - он 100% хочет опустошить ваш счет.

СРАЗУ КЛАДИТЕ ТРУБКУ, ЕСЛИ ЗВОНЯЩИЙ ПРОСИТ ЛОГИН/ПАРОЛЬ ОТ ИНТЕРНЕТ-БАНКИНГА ИЛИ ДАННЫЕ ИЗ СМС

Многофакторная (двухэтапная) аутентификация

Это дополнительная защита. То же самое, что второй замок на двери, ключ от которого находится в другой связке.

Если вы включите ее (во вкладках «Настройки», «Конфиденциальность»), то приложение будет просить не один пароль, а два (или даже больше).

Вход в аккаунт станет дольше, но на сегодня это самая работающая защита - убережет от 99% распространенных атак.

ВКЛЮЧИТЕ МНОГОЭТАПНУЮ АУТЕНТИФИКАЦИЮ

#### Фальшивый сайт

Это интернет-страница, повторяющая оформление настоящей. Вот только данные, которые вы вводите на ней, идут прямиком в руки мошенников.

Визуально заметить подмену сложно, но есть характерные маркеры:

- замочек слева от адресной строки не замкнут или есть надпись «Не защищено»;

- электронный адрес ненастоящий или буквы в нем перепутаны (bel-post.by вместо belpost.by, bealrusbank.by вместо belarusbank.by).

ВНИМАТЕЛЬНО СМОТРИТЕ НА АДРЕСНУЮ СТРОКУ САЙТА

#### Удаленный доступ

Мошенники просят установить из Google Play или App Store приложение (чаще всего - AnyDesk или TeamViewer, но есть и другие) и с его помощью получают доступ к чужому гаджету. Они смогут увидеть и записать все логины/пароли/коды, которые вы вводите в соцсетях, интернет-банкинге.

ОТКАЖИТЕСЬ, ЕСЛИ НЕЗНАКОМЕЦ ПРОСИТ ВАС УСТАНОВИТЬ КАКОЕ-ЛИБО ПРИЛОЖЕНИЕ

#### Защита от лишних звонков

Откройте «Вайбер» на телефоне, вой­дите в раздел «Еще» (правый нижний угол) и выберите вкладку «Настройки». Нажмите на «Вызовы и сообщения» и активируйте пункт «Защита от лишних звонков». Если такой строчки нет - обновите «Вайбер».

Теперь вы не будете получать звонки от неизвестных контактов (они автоматически получат пометку «пропущенный»).

АКТИВИРУЙТЕ ЗАЩИТУ ОТ ЛИШНИХ ЗВОНКОВ СЕБЕ И БЛИЗКИМ

### Топ-8 грязных схем

#### ЗВОНОК ИЗ БАНКА

Звонящий представляется сотрудником службы безопасности банка и уверяет: «С вашей карты кто-то хотел похитить деньги, для отмены операции назовите свои данные». Выманив сведения, мошенник выводит со счета все средства и исчезает.

Как не попасться? Скажите, что вы не клиент этого учреждения (даже если это так). Если на той стороне мгновенно переключат на «специалиста из вашего банка» - это точно мошенничество.

Или просто положите трубку и перезвоните в банк сами. Только номер телефона смотрите не во «Входящих», а на сайте.

#### СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

Мошенники в соцсетях создают группу якобы с целью сбора средств на лечение тяжелобольного. Деньги предсказуемо забирают себе.

Как не попасться? Запросите у администратора группы справки, документы, другие дополнительные сведения.

#### ПИСЬМО ОТ ДРУГА

Преступник взламывает чужие соцсети и рассылает друзьям пользователя сообщения с просьбой сбросить денег или отправить откровенные фото. Мошенник заранее изучает переписку жертвы и выбирает максимально похожий стиль письма.

Как не попасться? Позвоните другу и уточните, действительно ли он вам пишет. Если нет возможности позвонить - напишите в другом мессенджере.

#### ДЕШЕВЫЕ ВЕЩИ

Вор создает в социальной сети (чаще - в Instagram и «ВКонтакте») страницу якобы интернет-магазина с подозрительно низкими ценами. Когда жертва вносит предоплату или перечисляет всю стоимость товара, то оказывается в «черном списке» и больше не может связаться с продавцом.

Как не попасться? На странице найдите реквизиты продавца (как минимум, УНП, который должен указываться обязательно) и проверьте их на сайте kartoteka.by, поищите отзывы через поисковик. Настаивайте на отправке с наложенным платежом (оплата при получении).

#### АРЕНДА КВАРТИР

Выставив низкую цену за аренду квартиры, мошенник ждет откликов. В переписке уверяет: интерес большой, чтобы оставить бронь - внесите предоплату. Дальше два пути: или бросает фейковую страницу и сразу крадет введенные данные карты, или дает реальные реквизиты своего пластика (усыпляет бдительность). Во втором случае будьте готовы получить сообщение об отмене сделки с извинениями и просьбой прислать информацию о счете якобы для возврата средств.

Как не попасться? Настаивайте на личной встрече для передачи денег под расписку.

Еще одна простая проверка - попросить созвониться: фальшивые «арендодатели» под разными предлогами избегают живых разговоров.

#### ЗАНЯТОЙ ПОКУПАТЕЛЬ

Человек активно интересуется товаром на торговой площадке (том же «Куфаре») и просит либо отправить посылку курьером (тяжело нести с почты/не может отлучиться с работы), либо прямо сейчас принять предоплату на карту. Следом в переписку летит фишинговая ссылка, где нужно указать данные карточки.

Как не попасться? Откажитесь от таких форм оплаты/доставки.

Не вводите данные карты (особенно - срок действия и CVV-код) на сайтах, куда перешли по ссылкам от незнакомцев. Не соглашайтесь уходить с торговой площадки и продолжать переписку в другом приложении.

#### РОЗЫГРЫШИ И ЛОТЕРЕИ (=ОТДАМ ДАРОМ)

На почту или в личку приходят письма вроде «Вы сделали репост и выиграли приз!». Или кто-то на сайте-барахолке обещает отдать даром дорогой гаджет. Следом - условия получения: надо указать паспортные данные и заплатить за доставку (страховку).

Как не попасться? Не переходите ни по каким ссылкам из письма (даже если они якобы ведут к результатам игры). Через поисковик узнайте, действительно ли розыгрыш был проведен, есть ли другие призеры.

#### МНЕ ТОЛЬКО ПОЗВОНИТЬ

Человек просит ваш телефон срочно позвонить кому-то, потому как у него сел аккумулятор. Получив мобильный, мошенник быстро устанавливает на него следящее приложение. Как только вы решите войти в интернет-банкинг, вор перепишет данные и опустошит счет или прямо в личном кабинете возьмет кредит.

Как не попасться? Лучше вовсе не давать свой смартфон кому-то. Или набирайте номер сами и блокируйте экран, когда будете передавать гаджет для разговора.

<https://mvd.gov.by/ru/news/8099>