

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЖИЗНЕДЕЯТЕЛЬНОСТИ: ОТ КИБЕРАТАК ДО ПРАВИЛ НА ДОРОГАХ



Одной из важнейших государственных задач является системная работа по формированию культуры безопасности жизнедеятельности населения. **От уровня знаний, ответственности и осознанности каждого гражданина напрямую зависят его личная безопасность, благополучие общества и устойчивое развитие государства.**

Цифровая безопасность

В современном высокотехнологичном мире, когда киберпреступники разрабатывают все более изощренные и сложные методы атак, безопасность человека приобретает особую значимость.

Современное мошенничество – это уже не только история про пожилого человека, которому позвонили по телефону. Это проблема, с которой сталкиваются люди разных возрастов, разных профессий, с разным, порой очень высоким, уровнем образования и разным опытом пользования Интернетом.

Доля киберпреступлений каждый год увеличивается и уже составляет более трети от всех зарегистрированных преступлений в Беларуси.



Справочно:

По данным Министерства внутренних дел Республики Беларусь, если в 2023 году доля киберпреступлений составила 21,5% от всех зарегистрированных преступлений в стране, то в 2024 году – 27,5%, в 2025 году – 29,7%, а за 5 месяцев 2026 года – 33,4%.

В 2026 году еженедельно в стране совершается около 359 киберпреступлений, каждый день – более 50. При этом в возрастной структуре потерпевших преобладают лица молодого возраста: на группу лиц 18–29 лет пришлось 29,3% киберпреступлений.

По способам совершения киберпреступлений лжепродажа товара онлайн в текущем году занимает лидирующее место по количеству фактов (37,6%), второе место – вишинг от имени должностных лиц (33,8%), на третьем месте – хищение с использованием социальных сетей (9,7%).

Бдительность и внимательность – главный барьер против кибермошенников. Чтобы не стать жертвой, всегда критически оценивайте любые сообщения и звонки, поступающие с незнакомых номеров.

Справочно:

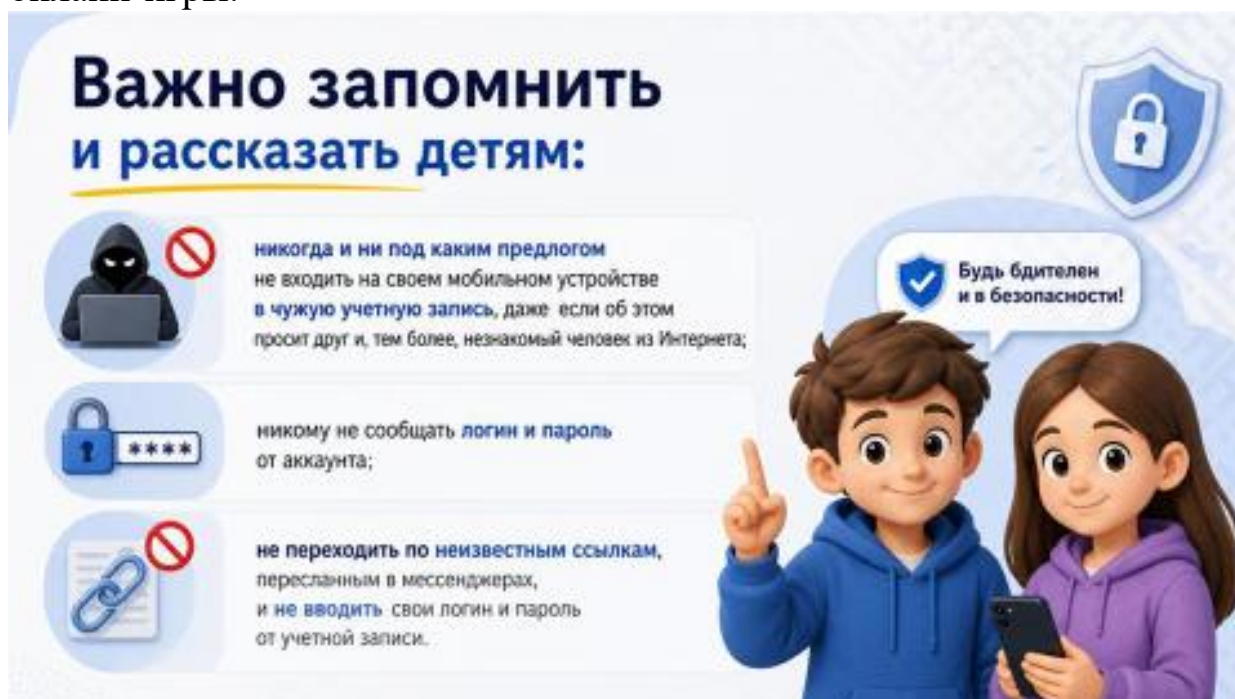
В Беларуси приняты дополнительные меры для защиты от вывода мошенниками денежных средств со счетов в банках. Например, с 1 июля 2026 г. банки обязаны соблюдать новые требования по сбору, хранению и анализу «цифрового отпечатка» устройства (т.наз. антифрод-система), в том числе о его геолокации. Это позволяет вовремя заметить подозрительную активность в интернет-банкинге и не допустить, чтобы мошенники похитили деньги клиента. Помните: это делается для защиты потребителя. **Геолокация – для вашей безопасности!**

Сегодня Интернет стал неотъемлемой частью жизни подрастающего поколения. Из-за недостатка жизненного опыта и

цифровой грамотности **жертвами кибермошенников часто становятся дети**. Особенно сейчас, в период летних каникул, когда большую часть свободного времени молодежь проводит в сети.

Несмотря на уменьшение преступлений, совершенных несовершеннолетними с использованием информационно-коммуникационных технологий, за 5 месяцев текущего года наблюдается **рост количества несовершеннолетних (+69,6%; с 158 до 268), признанных потерпевшими от киберпреступлений**.

На сегодняшний день **одна из самых распространенных схем, используемых злоумышленниками, – блокирование мобильных устройств Apple с последующим требованием определенных сумм за разблокировку**. Чаще подобные ситуации возникают через сетевые онлайн-игры.



Нередко аферисты используют платформы, сервисы для знакомств в онлайн-пространстве. При общении собеседник-мошенник говорит о том, что у него якобы сломался телефон. Даже присылает фотографию сломанного, разбитого гаджета. Жалуется, что у него в «облаке» остались курсовая, фотографии, которые необходимы, и просит свою жертву зайти в его iCloud и скачать необходимую информацию. А дальше – блокировка телефона и требование денег.

Кроме того, небезопасны и переходы по фишинговым ссылкам, например, при покупке товаров.

Мошенники также **используют детей в схемах против взрослых**. Несовершеннолетнему могут позвонить от имени мобильного оператора якобы для заключения договора, а затем потребовать сообщить код.

Потом перезванивает мошенник и говорит, что ребенок участвует в преступной схеме. Он или его родители могут быть привлечены к уголовной ответственности. Заставляют передавать курьеру определенные денежные суммы, дабы погасить кредиты, которые якобы были уже оформлены. И дети могут вынести из дома деньги и передать курьерам.



Кроме того, в сети Интернет также происходит **вовлечение детей в незаконный оборот наркотиков**, начиная от их вербовки, обучения и заканчивая передачей денег. Для недопущения подобного необходимо принимать меры по отслеживанию активности своих детей в сети Интернет, знать с кем они переписываются, что ищут с помощью поисковых систем. Для этого существуют различные программы родительского контроля, которые бесплатно можно установить на мобильный телефон, ноутбук или компьютер.

Важно знать: в большинстве случаев мошенник не взламывает телефон, не вскрывает квартиру и не получает доступ к деньгам силой. Он делает так, чтобы человек сам выполнил нужное действие: сообщил код, перешел по ссылке, ввел данные карты, оформил кредит, перевел деньги, установил приложение или передал доступ к аккаунту.

Поэтому главная защита – не только антивирус, пароль или сложные технические настройки. Главная защита – **умение вовремя распознать ситуацию, остановиться и не выполнять указания неизвестного человека.**