



# Вестник здорового образа жизни



Информационный бюллетень отдела общественного здоровья

## Стоп кибермошенникам!

**Э**лектронные сервисы, интернет-банкинг, удаленная работа и учеба, социальные сети, интернет-магазины и маркетплейсы – все это настолько прочно вошло в нашу повседневность, что иногда трудно поверить, как жили без этого раньше. Чем больше мы погружаемся в мир информационно-коммуникационных технологий, тем уязвимее становимся для интернет-преступников.

Киберпреступность идет в ногу со временем, с развитием технологий меняются схемы и способы обмана. Отдельное беспокойство вызывает **применение искусственного интеллекта** в преступной деятельности.

Наиболее распространенным способом интернет-хищения денежных средств является **телефонное мошенничество** в различных модификациях. Аферисты представляются работниками банков, коммунальных служб, водоканала, энергонадзора, служб газа и связи, сотрудниками правоохранительных и государственных органов, даже знакомыми и родственниками. Чтобы похитить деньги мошенники под различными предлогами пытаются завладеть личными данными, включая коды из смс. Часто они действуют в паре. Например, первый под предлогом замены ключей от домофона выманивает числовой код из смс, а второй, представляясь правоохранителем, угрожает проведением обыска и изъятием денежных средств за передачу того самого кода. Или один мошенник представляется руководителем вашей организации и пугает подозрением в экстремистской деятельности и проведением обыска, а другой от имени правоохранителя предлагает якобы помощь в решении данной проблемы: для этого нужно перевести деньги на «временный счет» или передать их курьеру.



**Никаких временных счетов не бывает и вернуть свои деньги с чужого счета невозможно.**

**Нельзя выполнять никаких действий, связанных с финансами, по указанию незнакомых, кем бы они не представились.**

Больше всего людей становятся жертвами киберпреступников при попытке купить товар подешевле в социальных сетях или мессенджерах. Часто в мошеннических аккаунтах «продают» одежду, смартфоны, автомобильные шины, садовые кресла, цветы и многое другое, то, что нужно доставлять курьером, а не почтой.

**Остерегайтесь подозрительно низких цен и не переводите предоплату за товар или услугу, выбирайте оплату наложенным платежом. Прежде чем согласиться на покупку, проверьте наличие у продавца сайта в белорусском сегменте интернета и созвонитесь с ним по телефону. Тщательно проверяйте информацию о продавце.**

Также хищения мошенники совершают с использованием поддельных инвестиционных или криптовалютных платформ. Размещая рекламу в Интернете, они могут использовать видео с известными людьми – политиками, спортсменами, блогерами, которые озвучены фразами, сгенерированными с помощью искусственного интеллекта. Например, на видео может быть известная телеведущая, которая в репортаже рассказывает о якобы новой возможности заработка, или заместитель министра дает интервью, что многие уже пользуются определенным ресурсом и получают деньги, хотя на самом деле все слова – это всего лишь результат работы нейросетей. С заинтересованными связываются так называемые кураторы или брокеры и убеждают участвовать в инвестировании или программе на том самом ресурсе. Для получения пассивного дохода предлагают вложить деньги в прибыльный проект. Часто жертв побуждают к оформлению кредитов для перевода большей суммы. На самом деле вкладчику просто «рисуют» его прибыль на сайте и никогда не дают возможности вывести его деньги.

**Нужно понимать, что легких денег не бывает, а бесплатный сыр в мышеловке. Вернуть деньги, «вложенные» подобным образом, невозможно.**

Одним из новых, набирающих обороты, способов является вымогательство за разблокировку Iphone. Вначале аферист в переписке узнает о наличии Iphone у будущей жертвы, а потом под различными предлогами убеждает войти в его iCloud. После этого Iphone жертвы блокируется. Для его разблокировки предлагается заплатить сумму, в зависимости от модели, превышающую 1000 рублей.

**Чтобы не стать жертвой киберпреступников, необходимо всегда адекватно оценивать свои действия и как бы вас не запугивали, не поддаваться панике и страху. Будьте бдительны и берегите свои деньги!**