



КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЯ?

1. **Никогда, никому и ни при каких обстоятельствах не сообщать реквизиты своих банковских счетов и банковских карт**, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов, при отсутствии возможности достоверно убедиться, что эти люди те, за кого себя выдают.

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк.

Необходимо принимать во внимание, что реальному сотруднику банка известна следующая информация: фамилия держателя карты, паспортные данные, какие карты оформлены, остаток на счете.

Не следует сообщать в телефонных разговорах (даже сотруднику банка), а также посредством общения в социальных сетях: полный номер карточки, срок ее действия, код CVC/CVV (находящиеся на обратной стороне карты), логин и пароль к интернет-банкингу, паспортные данные, кодовое слово (цифровой код) из SMS-сообщений.

В случае если «сотрудник банка» в разговоре сообщает, что с карточкой происходят несанкционированные транзакции, необходимо отвечать, что вы придете в банк лично, – все подобные вопросы нужно решать в отделении банка, а не по телефону.

ВНИМАНИЕ: *помните, что сотрудники банковских учреждений никогда не используют для связи с клиентом мессенджеры (Viber, Telegram, WhatsApp).*

2. Для осуществления онлайн-платежей необходимо использовать только надежные платежные сервисы, **обязательно проверяя доменное имя ресурса в адресной строке браузера.**

3. **Не следует хранить банковские карты, их фотографии и реквизиты в местах, которые могут быть доступны посторонним лицам;** это же относится к фотографиям и иным видам информации конфиденциального характера.

4. Следует **воздерживаться от осуществления онлайн-платежей, связанных с предоплатой и перечислением задатков за товары и услуги, благотворительной и спонсорской помощи в пользу организаций и физических лиц** при отсутствии достоверных данных о том, что названные субъекты являются теми, за кого себя выдают.

5. Не стоит перечислять денежные средства на счета электронных кошельков, карт-счета банковских платежных карточек, счета SIM-карт **по просьбе пользователей сети Интернет.**

6. Для доступа к системам дистанционного банковского обслуживания (интернет-банкинг, мобильный банкинг), электронным почтовым ящикам, аккаунтам социальных сетей и иным ресурсам **необходимо использовать сложные пароли, исключая возможность их подбора.** Стоит воздержаться от паролей: дат рождения, имен, фамилий – то есть тех, которые легко вычислить из общедоступных источников информации (например, тех же социальных сетей).

7. При составлении платежных документов **важно проверять платежные реквизиты получателя денежных средств.**

8. При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек **не следует отвечать на подобные сообщения, а необходимо связаться с данными пользователями напрямую посредством иных средств связи.**

9. При обнаружении факта взлома аккаунтов социальных сетей необходимо незамедлительно восстанавливать к ним доступ с помощью службы поддержки либо блокировать, а также предупреждать об этом факте лиц, с которыми общались посредством данных социальных сетей.

10. **Нельзя открывать файлы, поступающие с незнакомых адресов электронной почты и аккаунтов мессенджеров;** не переходить по ссылкам в сообщениях о призах и выигрышах.

11. Необходимо **использовать лицензионное программное обеспечение, регулярно обновлять программное обеспечение и операционную систему; установить антивирусную программу** не только на персональный компьютер, но и на смартфон, планшет и регулярно обновлять ее.

12. Следует **ознакомить с перечисленными правилами безопасности своих родственников и знакомых,** которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

Как дети могут стать киберпреступниками?

С каждым годом интернет-мошенники и взломщики становятся все моложе. Современные подростки проводят в интернете большую часть своего времени, но возможности Всемирной паутины каждый использует по-разному. Около 92% родителей Беларуси не знают о потенциально опасных активностях своих детей в интернете. При этом 58% несовершеннолетних скрывают от родителей, чем на самом деле они занимаются в сети. Самым распространенным способом интернет мошенничества среди несовершеннолетних – использование банковских карт родителей (других членов семьи) при покупке донат.

Донат - в онлайн играх обычно обозначает оплату игроком дополнительных бонусов, уникальных предметов и прочих благ, не доступных обычным путем, без оплаты реальными деньгами. Чаще всего, в чистом виде, донат встречается в бесплатных играх — увеличенная скорость прокачки, уникальная и мощная экипировка, хитрая валюта за которую можно купить в игре что-то ядреное, вкусности, оружие и т.д. В платных же играх, как например WOW, под донатом подразумевается приобретение уникальных питом (животные, существа, привязанные к персонажу и сопровождающие его в игре) и маунтов (средство передвижения), доступных в игре только за наличные деньги.

Многие родители не зная, что их ребенок геймер тратит свои карманные деньги на донат игр, становиться зависим от этого. Ребёнок геймер донатит, чтобы казаться лучше других игроков и иметь преимущество над ними в игре.

Дети нарушают ч2 ст.212 и ч.2 ст.349 Уголовного Кодекса РБ.