**ОСНОВЫ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ**

Если Вам поступил звонок «лжесотрудника» банковских учреждений следует помнить:

• ни при каких обстоятельствах, никому и никогда не сообщайте информацию о себе или своей банковской платежной карте. Если Вам будет звонить настоящий сотрудник банка, то он точно будет знать, как минимум номер Вашей банковской платежной карты и никогда не спросит конфиденциальную информацию в телефонном режиме;

• уточните с кем именно Вы общаетесь, после чего положите трубку и перезвоните на номер телефона, который отображался у Вас на экране (в этом случае Вы свяжитесь именно с тем абонентом, которому принадлежит указанный номер, а не со злоумышленниками, которые его использовали с целью скрыть свой настоящий номер) и уточните суть возникшей проблемы;

• если же на Вас оказывается психологическое давление угрозами, что через несколько секунд Вы понесете финансовые потери, кто-то оформит на Вас кредит или что если Вы не сообщите требуемую информацию, то карту вообще заблокируют, не волнуйтесь, это обычная уловка преступников, главная цель которых ввести Вас в состояние неуверенности и страха потерять сбережения;

• сами перезвоните в свой банк или в круглосуточную службу сервиса, номер

которой написан на оборотной стороне Вашей платежной карты и сообщите о случившемся.

!!!!!Помните, если Вы сообщите злоумышленнику реквизиты своей банковской платежной карты, то он сможет распоряжаться всеми средствами на счету, а также оформить на Ваше имя дополнительные кредитные обязательства (онлайн-кредит)

Как не стать жертвой киберпреступников, совершая сделки в сети Интернет

• вести общение с потенциальными покупателями или продавцами только во внутреннем чате торговой площадки (зачастую торговые площадки блокируют возможность перехода на поддельные ресурсы); • ведя общение с пользователем стоит перейти к его профилю и обратить внимание на дату создания (если он создан несколько дней назад, то это должно вызвать дополнительную настороженность);

• очень внимательно относится к любому случаю, когда необходимо ввести данные карты или информацию, предоставленную банком (смс-код, логин или пароль от интернет-банкинга); • уточнить у собеседника номер телефона если он не указан в объявлении, а потом позвоните на этот номер, чтобы убедиться, что он реален и принадлежит именно пользователю, с которым вы совершаете сделку;

• использовать отдельную банковскую карту для осуществления покупок в сети Интернет, на которой не хранятся денежные средства и на которую не поступает регулярный доход в виде заработной платы, стипендии или пенсии; • избегать перехода по неизвестным интернет-ссылкам, которые предоставляются в ходе переписки якобы для получения предоплаты или оформления доставки.

!!!!Соблюдение этих несложных мер предосторожности позволит уберечь ваши денежные средства от преступных посягательств!!!!

Типичные действия злоумышленника после несанкционированного доступа к чужим аккаунтам

рассылка всем виртуальным «друзьям» потерпевшего просьбы под

различными предлогами сообщить реквизиты банковской платежной карты. Это может быть ее фото или просто номер, срок действия и иные реквизиты;

изучение содержания переписок потерпевшего и использование их содержания в качестве инструмента для вымогательства денежных средств (личные диалоги на откровенные темы, фотографии, содержащиеся на странице и в диалогах и иные очень личные данные);

Рассылка различного рода порочащей информации от имени владельца страницы иным пользователям, ссылок на поддельные ресурсы банковских учреждений, а также вредоносное программное обеспечение !!!!

В случае обнаружения «взлома» аккаунта, прежде всего следует попытаться восстановить доступ к нему путем отправки сообщения на «привязанный» номер мобильного телефона или электронную почту,

оповестить друзей и знакомых об инциденте, используя при этом иные соцсети и мессенджеры !!!!

Правила информационной безопасности:

Не устанавливать программное обеспечение из неизвестных источников.

Не открывать электронных писем от неизвестных отправителей, не переходить по ссылкам и не запускать вложенные файлы

Использовать наиболее современную версию антивирусного программного обеспечения

Хранить пароли в тайне от близких

Не осуществлять переходов по подозрительным ссылкам и не вводить личную информацию (номера карт, телефонов и т.п.)