Уважаемые граждане!

Уведомляем Вас о том, что по-прежнему совершение преступлений с использованием информационно-коммуникационных технологий продолжают прогрессировать и злоумышленники путем различных методов и способов завладевают денежными средствами.

Самыми распространенными киберпреступлениями являются: **Вишинг** (англ. vishing, от voice phishing) - один из методов мошенничества с использованием социальной инженерии, который заключается в выведении злоумышленников жертвы на желаемую модель поведения с целью завладения конфиденциальной информации для последующего хищения средств (пример: **«Звонок из банка»**).

Фишинг (от англ. ,Fshing рыбная ловля, выуживание) — один из видов мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам и паролям) и последующего хищения денежных средств. Наиболее часто данная преступная схема реализовывает в отношении клиентов торговых интернет-площадок. Выступая в роди покупателя, злоумышленник находит продавца товара и вступает с ним в переписку в мессенджерах («Viber», «Telegram», «WhatsApp»), Он сообщает, что товар его заинтересовал и уже якобы совершил предоплату (зачастую высылается скриншот электронного чека о перечислении средств), Для того, чтобы получить данные средства, продавцу якобы необходимо пройти по и ввести данные.

Ко всему прочему, в настоящее время участились способы мошенничества путём представления оператором сотовой связи. В ходе диалога злоумышленники предлагают продлить договор или установить мобильное приложение оператора сотовой связи, которое является фишинговым, в следствии чего они получают доступ ко всем Вашим данным, включая банковские счета, в случае, если у вас установлено приложение банка, либо выполнен вход в м-банкинг через браузер.

Также при пользовании торговыми площадками такими как «Kufar», «Ozon», «Onliner» и т.п. будьте внимательны с предоставлением ваших личных данных в ходе диалога с продавцом, так как в этом случае вы можете стать жертвой мошенничества. Ни в коем случае не предоставляйте в ходе переписки в чате номера Ваших банковских карт, CVV/CVC коды(находящиеся на оборотной стороне банковской карты), а также Ваши паспортные данные.

В некоторых случаях злоумышленники могут угрожать разглашением различных компрометирующих сведений с целью вымогательства,

Социальные сети — это кладезь персональной информации о человеке. Получив несанкционированный доступ к страницам в социальных сетях, переписке электронных почтовых ящиков и облачным аккаунтам и завладев изображениями, не предназначенными для публичного просмотра,

преступники вступают в переписку с потерпевшими, требуя разные денежные суммы и угрожая в случае отказа распространить их в сети Интернет.

«Алло мама»- злоумышленники звонят и говорят о горестной вести о нахождения какого-либо из родственников в критической ситуации (пострадал в ДТП, возбуждено уголовное дело и для решения вороса необходимо уплатить значительную сумму и д.р.)

Основные ПРАВИЛА

Никогда, никому и ни при каких обстоятельствах не сообщайте реквизиты своих банковских счетов и банковских карт, в том числе лицам, представившимся сотрудниками банка или правоохранительных органов.

Также не следует сообщать в телефонных разговорах и при общении в соцсетях 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

В случае поступления звонка «от сотрудника банка» необходимо уточнить его фамилию, номер телефона, после чего завершить разговор и самим позвонить в банк или в круглосуточную службу сервиса, номер которой написан на оборотной стороне платежной карты.

Учтите: сотрудники банков или операторов сотовой связи никогда не используют для связи с клиентами мессенджеры («Viber», «Telegram», «WhatsApp»).

Ни в коем случае не предоставляйте доступ к мобильному устройству посторонним лицам!

Никогда не устанавливайте по просьбам незнакомых лиц, программы удаленного доступа, такие, например, как «AnyDesk», «TeamViewer», «RustDesk» и др. Несообщайте незнакомым лицам сеансовые коды! Через эти приложения мошенники могут получить доступ к мобильному приложению интернетбанкинга на Вашем устройстве и совершить хищение денежных средств.

Для доступа к системам дистанционного банковского обслуживания и личным аккаунтам необходимо использовать сложные пароли, исключающие возможность их подбора.

При поступлении в социальных сетях сообщений от лиц, состоящих в категории «друзья», с просьбами о предоставлении реквизитов банковских платежных карточек не следует сразу же отвечать на подобные сообщения!

Нередко такие просьбы рассылаются от имени друзей преступниками, взломавшими аккаунт в социальной сети и получившими доступ к конфиденциальной переписке. Поэтому сначала необходимо связаться-р этим человеком (по телефону, лично встретиться) и уточнить, действительно ли он нуждается в помощи.

Обязательно расскажите об этих основных правилах «цифровой гигиены» своим родственникам, близким, знакомым и друзьям, ведь в силу возраста или недостаточного уровня финансовой грамотности они могут быть особенно уязвимы для действий киберпреступников!