МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГБПОУ РД «КОЛЛЕДЖ ЭКОНОМИКИ И ПРАВА»

ОТЧЕТ
о проведении классного часа
группы 19 ИСП 2
кл. руководитель - Наджафова А.С.

октябрь 2024

КЛАССНЫЙ ЧАС

Стартовала информационно-разъяснительная кампания по киберграмотности «Клади трубку»!

Они постоянно придумывают все более изощренные схемы и сценарии для звонка, чтобы заполучить доступ к деньгам. Схемы злоумышленников часто выглядят очень правдоподобно, так как они используют самые обсуждаемые новости или события. Чтобы вызвать доверие, они могут обращаться по имени и отчеству. С первых минут разговора мошенники начинают давить авторитетом и должностью. Следуя общим правилам поведения с кибермошенниками, вы сможете себя обезопасить:

− не сообщайте никому личные (данные паспорта, ИНН, дату рождения, адрес места жительства и другие) и финансовые (номер, срок действия, трехзначный код с оборотной стороны карты) данные. Переданные мошенникам личные и финансовые данные могут быть использованы как для самого хищения, так и для оформления кредитов, передачи третьим лицам и для других противоправных действий;

− установите антивирусные программы на все свои гаджеты. Данное ПО предупредит вас в случае установки подозрительного продукта на ваш гаджет. Важно регулярно обновлять антивирусную базу.

− не читайте сообщения и письма от неизвестных адресатов и не перезванивайте по неизвестным номерам. Подобные письма могут содержать в себе вредоносное ПО или фишинговую ссылку, а звонки на неизвестные пропущенные телефонные номера могут быть чреваты как минимум списанием значительной суммы с вашего мобильного счета, а как максимум − быть поводом для мошенников активизировать против вас мошенническую схему;

− не переходите по сомнительным ссылкам и не скачивайте неизвестные файлы или программы. Сомнительные ссылки могут быть опасны для вашего гаджета наличием вируса или вредоносного ПО на сайте, на который они ведут, а скачивание программ с неофициальных источников может дать мошенникам доступ к вашему гаджету;

− заведите отдельную банковскую карту для покупок в Интернете. Перед покупкой переводите на нее ровно ту сумму, которая нужна. Даже если мошенники получат доступ к этой карте, они не смогут похитить больше тех средств, которые были на ней.


Как распознать мошенника?
Просят данные банковской карты, пароли и коды из СМС
Предлагают перевести деньги на «безопасный счет»
Гарантируют супердоход от инвестиций
Представляются якобы сотрудниками банка или полиции
Пугают взломом Госуслуг
Клади трубку
Без разговоров.
Это мошенники!
Банк России
МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ