В апреле 2023 года в МБОУ «Лицей № 57 имени Героя Советского Союза А.А. Бельгина» в старшем образовательном звене (9-11-е классы) была проведена квест-игра «Социальные инженеры»: как не попасться в ловушку кибермошенников». Ребята искали ответ на вопрос: «Какие способы обмана применяют мошенники и как этому можно противостоять?». Конечным результатом данной игры стала разработка и распостранение старшеклассниками листовок.

**ВНИМАНИЕ !! КИБЕРМОШЕННИЧЕСТВО !!!!**

**ВИРУС**

Вирусы могут открыть удаленный доступ к вашему устройству, украсть логины и пароли от онлайн- и мобильного банка, а также перехватывают секретные коды из сообщений. Заполучив эти данные, киберпреступники могут похитить все деньги с ваших счетов.

**Онлайн-мошенник**

Стать жертвой мошенника можно не только на улице. С развитием технологий охотники за наживой быстро освоили и виртуальное пространство. Аферисты могут подстерегать своих жертв на самых разных онлайн-площадках: они нередко играют роль покупателей или продавцов на интернет-сервисах для размещения объявлений о товарах и услугах, копируют известные сайты, присылают подозрительные ссылки через социальные сети, мессенджеры или на электронную почту.

**ПОДМЕННЫЕ НОМЕРА**

Киберпреступники научились маскировать свой телефонный номер под официальные номера банков. Разбираемся, как не попасться на уловки мошенников. Главное – помнить: даже если у вас на телефоне высветился знакомый номер банка, ни в коем случае не делайте на него обратный звонок. Наберите номер горячей линии банка вручную. Телефон горячей линии можно найти на обратной стороне банковской карты или на официальном сайте банка.

**С КАРТЫ УКРАЛИ ДЕНЬГИ**

Пришло СМС, что с карты списали деньги, но вы ничего не покупали, переводы не делали и наличные не снимали. Вероятно, ваша карта или ее данные попали к мошенникам. В такой ситуации нужно немедленно заблокировать карту, сообщить в банк по горячей линии о краже денег и написать в отделении банка заявление о несогласии с операцией. Сделать все это необходимо не позднее следующего дня после того, как банк уведомил вас об операции, которую вы не совершали.

**ТЕЛЕФОННЫЕ МОШЕННИКИ**

Вам позвонили на мобильный с незнакомого номера. Солидный мужской голос на фоне шума офиса сообщил: «Это служба безопасности вашего банка. Мы зафиксировали, что киберпреступники пытаются получить доступ к вашему личному кабинету. Надо срочно перевести все деньги на безопасный счет, иначе их украдут!». В такой ситуации нужно немедленно положить трубку: это звонят мошенники. Аферисты постоянно придумывают новые способы выманить у людей деньги или конфиденциальные данные для доступа к счетам.

**ФИШИНГ**

Фишинг – главное оружие киберпреступников. Другими словами – это выуживание конфиденциальных данных: паролей, реквизитов карты или счета для кражи денег с карты или из интернет-кошелька. Воры играют на психологии: рассылают СМС, электронные письма и сообщения в чатах с просьбой, например, «подтвердить аккаунт» или «восстановить доступ к банковскому счету». При этом сообщения содержат ссылку на специальный фишинговый сайт – сайт-двойник банка, госоргана или другой организации. Если вы не заметили подмены, то после ввода своего логина, пароля интернет-банка или реквизитов карты переведете деньги мошенникам.