КИБЕРПРЕСТУПНОСТЬ

КАК УГРОЗА СОВРЕМЕННОМУ ИНФОРМАЦИОННОМУ ОБЩЕСТВУ

Мошенничество

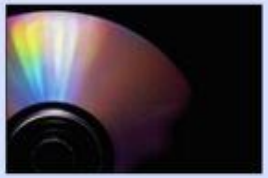
Мошенничество в интернете - один из видов киберпреступления, целью которого является обман пользователей.

СТРУКТУРА КИБЕРПРЕСТУПНОСТИ

Компьютерные преступления

Телекоммуникационные преступления

Незаконный оборот объектов интеллектуальной собственности



Незаконный оборот радиоэлектронных и специальных технических средств

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА

«ОНЛАЙН ПОКУПКИ»
Якобы продавец просит за товар предоплату либо полную оплату покупки, после чего связь с мошенником прекращается

«МЫ НАШЛИ ВАШИ ДОКУМЕНТЫ»
Якобы нашли ваши утерянные документы и просят вознаграждение за их возврат

«ПРИВЯЗКА КАРТЫ»
Просят привязать вашу банковскую карту к какому-либо номеру телефона или счету

«ВИРУСНАЯ АТАКА»
SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащая вредоносную программу, дающую доступ мошенникам к вашей банковской карте

«ВЫПЛАТА ПРОЦЕНТОВ»
Обещание больших процентов по вкладам под короткие сроки на различных интернет сайтах

«ПОКУПКА АВИАБИЛЕТОВ»
продажа липовых авиабилетов на мошеннических сайтах

ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН

ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИКОВ

Помните! Ни в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счету ни под каким предлогом!
Пользуйтесь только проверенными сайтами, на которых решили совершить какие-либо покупки!
Оплачивайте товар только после его получения!

БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

ВНИМАНИЕ!

ЦИФРОВАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

УСТАНОВИТЕ АНТИВИРУС НА ВСЕ ВАШИ УСТРОЙСТВА

НЕ переходите по ссылкам и письмам от незнакомцев, не нажимайте на картинки и кнопки

НЕ сообщайте свои персональные данные и данные банковской карты

НЕ верьте обещаниям внезапных выигрышей

НЕ указывайте личную информацию в открытых источниках

НЕ используйте одинаковые пароли для всех аккаунтов

Сохрани эту информацию и поделись с другими

FinGramota
Повышение финансовой грамотности населения

МОШЕННИКИ «НА КАРАНТИНЕ»: ВИШИНГ

ЛУЧШЕ НЕВЕЖЛИВО ПРЕРВАТЬ РАЗГОВОР, ЧЕМ ВЕЖЛИВО СООБЩИТЬ PIN-КОД КАРТЫ.

Сотрудники банка никогда не попросят у вас данные по карте. А чтобы убедиться, что звонок был от мошенников, нужно звонить на официальный номер вашего банка.

НЕ СПЕШИТЕ РАСКРЫВАТЬ ПЕРВОМУ ЗВОНЯЩЕМУ СВОИ ДАННЫЕ, В БАНКЕ ИХ ИТАК ЗНАЮТ.

Банки никогда не звонят сами, чтобы спросить по телефону: полный номер карточки; срок ее действия; CVC/CVV; логин и пароль к интернет-банкингу; кодовое слово, код из SMS-сообщения.

НЕ ПОДДАВАЙТЕСЬ ПАНИКЕ, ЕСЛИ ВАС ПОПЫТАЮТСЯ НАПУГАТЬ ТЕЛЕФОННЫЕ МОШЕННИКИ.

На паническое заявление о том, что с вашей картой серьезная проблема лучший ответ: «Сейчас позвоню или схожу в банк, чтобы проверить это лично». Будьте уверены – звонящий тут же отключится. Это очень распространенная уловка – напугать владельца карты.

Заключение

Киберпреступность и кибертерроризм являются объективным следствием глобализации информационных процессов и появления глобальных компьютерных сетей. С ростом использования информационных технологий в различных сферах деятельности человека растет и использование их в целях совершения преступлений.

Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей кибертеррористов. О безопасности надо думать сегодня, завтра уже может быть поздно.