



В современном мире информационных технологий, число IT-преступлений стремительно растет, включая киберсквоттинг, фишинг, мошенничество с кредитными картами и взлом баз данных. Эти преступления наносят серьезный ущерб как индивидуальным пользователям, так и крупным корпорациям. Основные риски, связанные с хищениями, включают утечку конфиденциальной информации, финансовые потери и разрушение репутации компаний.

Чтобы защититься от этих угроз, важно внедрить надежные методы кибербезопасности. Во-первых, регулярное обновление программного обеспечения и операционных систем помогает закрыть уязвимости, используемые злоумышленниками. Во-вторых, использование сложных паролей и двухфакторной аутентификации значительно затрудняет доступ к личным данным.

Чтобы не стать жертвой злоумышленников, необходимо соблюдать простые правила безопасного поведения и обязательно довести их до сведения родных и близких. Противостоять мошенникам возможно лишь повышенной внимательностью, здравым смыслом и бдительностью.

НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ИНТЕРНЕТ МОШЕННИЧЕСТВА	НАИБОЛЕЕ РАСПРОСТРАНЁННЫЕ СХЕМЫ ТЕЛЕФОННОГО МОШЕННИЧЕСТВА
«ОНЛАЙН ПОКУПКИ» Любой 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» Просит привязать вашу банковскую карту к какому-либо номеру телефона или счету «ВИРУСНАЯ АТАКА» SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащий 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 литовых авиабилетов на мошеннических сайтах ПРОСЬБА ПЕРЕВЕСТИ КАКУЮ-ЛИБО СУММУ ОТ ВАШЕГО ЗНАКОМОГО, АККАУНТ КОТОРОГО БЫЛ ВЗЛОМАН	«ВАША КАРТА ЗАБЛОКИРОВАНА» SMS-сообщение о якобы заблокированной банковской карте, для разблокировки которой требуется сообщить ПИН-код вашей карты, либо провести определенные действия с помощью банкомата «РОДСТВЕННИК В БЕДЕ» Требование крупной суммы денег для решения проблемы с якобы пострадавшим или больным родственником «ВЫ ВЫИГРАЛИ» SMS-сообщение о том, что вы стали обладателем и вам положен приз «ВИРУСНАЯ АТАКА» SMS-сообщение, содержащее ссылку на какой-либо интернет ресурс, содержащий вредоносную программу, дающую доступ мошенникам к вашей банковской карте «ВАМ ПОЛОЖЕНА КОМПЕНСАЦИЯ» Вам якобы положена компенсация за приобретенные ранее некачественные БАДы либо иные медицинские препараты, для получения которой вам необходимо оплатить какие-либо пошлины или проценты «ОШИБОЧНЫЙ ПЕРЕВОД СРЕДСТВ» просит вернуть деньги за ошибочный перевод средств, дополнительно ссылаясь на средства со счета по чужу УСЛУГА, ЯКОБЫ, ПОЗВОЛЯЮЩАЯ ПОЛУЧИТЬ ДОСТУП К SMS И ЗВОНКАМ ДРУГОГО ЧЕЛОВЕКА
ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ КИБЕРОШЕННИКОВ Помните! Не в коем случае не привязывайте свою банковскую карту к какому-либо телефону или счету и не под каким предлогом! Помните! Только проверенные сайты, на которых решите совершить какие-либо покупки! Оплачивайте товар только после его получения! БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!	ПОМНИТЕ! ЧТОБЫ НЕ СТАТЬ ЖЕРТВОЙ ТЕЛЕФОННЫХ МОШЕННИКОВ Помните! Если вам звонят и тревожными голосом сообщают, что ваш близкий попал в беду, либо вы выиграли приз, либо вам положена какая-либо компенсация, не верьте - это мошенники! Никогда не переходите по ссылкам, присланным в SMS-сообщениях с неизвестными номерами! Никому не сообщайте ПИН-код вашей банковской карты! БУДЬТЕ ВНИМАТЕЛЬНЫ И БДИТЕЛЬНЫ!

