**Как не стать жертвой киберпреступления.**

За последние несколько лет информационные технологии плотно внедрились в повседневную жизнь человека, позволяя совершать покупки через онлайн-магазины, оплачивать жилищно-коммунальные услуги через приложения мобильных банков, общаться с помощью социальных сетей с людьми, живущих на всей территории земного шара, не выходя из дома с помощью информационно-телекоммуникационной сети «Интернет».

Первоначально размещение информации в российском сегменте Интернета характеризовалось отсутствием каких-либо ограничений, которое было продиктовано не столько обеспечением гарантий конституционного права граждан на свободу информации, сколько недостаточностью необходимых технических возможностей проконтролировать качество информации в Рунете. Сеть «Интернет» как средство, через которое может быть осуществлено право на свободу выражения мнений, может выполнять данную цель только при условии, что государство возьмет на себя обязательства разработать эффективную политику для достижения всеобщего безопасного доступа к сети Интернет. Данная политика должна обеспечивать защиту прав и свобод человека и гражданина, не допускать распространения вредной информации, противоречащей международным требованиям. До недавнего времени в законодательстве Российской Федерации не было предусмотрено правовое регулирование распространения информации в сети Интернет и применялись нормы из реальной жизни, а не виртуальной. Доступность сети «Интернет» в России, а также увеличение возрастного диапазона ее пользователей поставило вопрос о регулировании распространения вредной и неправомерной информации на приоритетное место.

Новые технологии все чаще выступают средством совершения самого широкого круга преступлений, от хищений денежных средств с расчетных пластиковых карт, до угроз критической инфраструктуре страны и обеспечению ее безопасности.

Зачастую чтобы выудить личные данные граждан и завладеть в последующем их денежными средствами злоумышленники пользуются доверием людей, используют простые, но эффективные способы манипуляции, психологические навыки. Людям звонят рано утром, поздно вечером, нередко на выходных, надеясь застать врасплох. Преступники говорят уверенно, приводят «железные» доводы, сыплют профессиональной терминологией, запугивают своих жертв. Это может быть игра на родственных чувствах, боязнь потерять деньги или, наоборот, радость от их внезапного получения. В запасе у мошенников много историй, потому что они нацелены не просто на похищение какой-то конкретной суммы, а на получение доступа к счетам и картам в целом.

Распространение получила схема, когда по телефону собеседник представляется сотрудником банка, говорит о том, что сработала система безопасности, и в данный момент по карте клиента проводится подозрительная операция. Чтобы ее остановить, необходимо назвать, к примеру, кодовое слово или ПИН-код. В дальнейшем мошенники, применяя психологические манипуляции, давят на людей, стимулируют их к совершению определенных действий со счетом или карточкой, необходимых для похищения денежных средств. Зачастую гражданам на телефон присылают SMS-сообщения подобного содержания.

Очень популярны среди населения покупки в интернет-магазинах и на сайтах объявлений типа «Avito». При этом, нередко продавец просит перечислить ему аванс за товар либо его полную стоимость с карты на карту. После перевода мошенник, естественно, исчезает.

Для того чтобы не стать жертвой мошенников соблюдайте простые правила предосторожности:

- ни при каких обстоятельствах не передавайте и не сообщайте, в том числе посредством сети Интернет, мобильной связи свои персональные данные кому-либо, в том числе номера, ПИН-коды и другие реквизиты банковских карт; номер паспорта; логины и пароли доступа; коды, которые банк направляет вам в виде СМС-сообщений;

- старайтесь не передавать третьим лицам свою банковскую карту, сотовый телефон, иные технические устройства;

- при поступлении звонков от лиц, представляющихся сотрудниками банка и предлагающих совершить какие-либо операции по карте или счету или сообщить персональные данные, не спешите выполнять операции, навязываемые Вам собеседником. Помните, что работник банка никогда не спросит Ваши персональные сведения о карте. В этой связи лучше прекратите разговор и позвоните в службу техподдержки своего банка и следуйте ее инструкции. Для защиты денежных средств клиентов у банка есть вся необходимая информация. Необходимо также всегда иметь при себе телефонный номер кредитного учреждения, чтобы в любой момент проконсультироваться о подозрительных ситуациях. Аналогичным образом необходимо действовать при получении СМС-сообщений подобного содержания;

- при совершении покупок в Интернете будьте особенно осторожными и внимательными, старайтесь не перечислять деньги дистанционно, не убедившись в благонадёжности продавца, сдержанно относитесь к заманчивым предложениям и скидкам;

- соблюдайте бдительность и осторожность при использовании сети Интернет, старайтесь не разглашать персональные данные. Используя электронную почту, старайтесь не открывать подозрительные и сомнительные письма, содержащие ссылки на сторонние Интернет-ресурсы. Не устанавливайте неизвестные программы на Ваши «девайсы» и технические устройства.

Уважаемые граждане! Помните, что злоумышленники совершают преступления в основном пользуясь Вашей доверчивостью и неосмотрительностью.