**Осторожно: мобильные мошенники!**

Сегодня невозможно представить себе современного человека без сотового телефона.

Современный мобильный телефон сожжет рассказать о своем владельце практически все: с кем чаще всего общается, где проводит свободное время, кем работает, о семье и друзьях, и даже о состоянии банковских счетов.

Развитие сотовой связи не прошло мимо преступного мира. И если раньше чаше всего просто воровали аппараты, то сегодня используются более сложные криминальные схемы, потому что информация, которую содержит сотовый телефон, может стоить в десятки и сотни раз дороже, чем собственно «трубка».

Злоумышленники всегда стараются «сыграть» на любопытстве, беспечности, страхе или сострадании людей.

Существует несколько видов мобильных мошенничеств:

- мошенничество «на доверии» (сообщение о выигрыше приза, денежный бонус за подключение, блокировщики рекламы, просьба одолжить телефон на улице для звонка, просьба положить на счет деньги, если друг, родственник попал в беду, выманивание паролей, объявления купли-продажи на сайтах, «перезвони мне», «верните, пожалуйста, мои деньги»);

- технические способы кражи информации (атака «клонов», телефонные инфекции).

Как же не стать жертвой мобильных мошенников?

1. Не оставляйте ваш телефон без присмотра в общественных местах.
2. Обязательно установить пароль для разблокировки и доступа к данным.
3. Никогда не храните ценную информацию только в телефоне, дублируйте ее на компьютере или в блокноте.
4. Не покупайте телефоны, бывшие в употреблении, на рынках ив ларьках. Большая часть из них может быть украденной, и в случае опознания аппарата бывшим владельцем его могут у вас изъять. Если будет доказано, что вы покупали заведомо краденый телефон, то вам может грозить уголовное наказание.
5. Игнорируйте просьбы положить кому-то деньги на мобильный телефон, если не уверены на 100%, что к вам обращается знакомый человек.
6. Будьте предельно бдительными, пользуясь банковскими услугами, в которых задействован номер мобильного телефона:

- никогда и никому не сообщайте присылаемые вам пароли и коды подтверждения;

- зная номер вашей банковской карты и телефон, злоумышленники могут попытаться украсть деньги. Храните эту информацию от посторонних;

- Вам никогда не позвонят представители банка с просьбой сообщить код подтверждения или код подлинности карты (три цифры на обороте карты возле места для подписи). Если вам поступил такой звонок, немедленно вешайте трубку!

- не открывайте ссылки, не скачивайте прикрепленные файлы, которые пришли от неизвестных вам абонентов;

- игнорируйте сообщения типа «Перезвони мне», «Положи на этот номер сто рублей», пришедшие с незнакомых номеров;

Если вы поняли, что разговариваете с мошенниками и к тому же передали им пароль от банковской карты:

- прервите разговор, положите трубку;

- немедленно позвоните в контактный центр своего банка. Такие клиентские службы работают круглосуточно, звонки на них с мобильного телефона, как правило, бесплатны. С помощью оператора совершите блокировку карты и входа в личный кабинет;

- оставьте заявку на перевыпуск карты банком (иногда это можно сделать по телефону);

- ознакомьтесь с правилами защиты от мошенничества на сайте банка. Если вы очень быстро среагируете, то преступники не успеют перевести деньги, даже если получили от вас пароль.

1. Отправка СМС-сообщений на сервисные (так называемые короткие) номера чаще всего приводит к списанию средств. Если же это действительно необходимо, то попробуйте получить уточняющую информацию у вашего оператора сотовой связи, как будет тарифицирована отправка сообщения на данный номер телефона.
2. Никогда не сообщайте персональных данных (дату рождения, Ф.И.О., данные о родственниках и т.п.), кем бы не представлялся звонящий: сотрудником банка, полиции, менеджером мобильного оператора. Если вам кажется, что это «правильный» звонок, попросите представиться, назвать Ф.И.О., звание и должность, поинтересуйтесь, какой адрес у отделения, офиса. Затем следует узнать телефон этой организации в справочнике и самому перезвонить. Помните: мошенники могут использовать ваши персональные данные в разнообразных преступных схемах.
3. Вам могут позвонить и сообщить, что ваш родственник или знакомый попал в аварию, в отделение полиции, в больницу и за него нужно внести залог, штраф, взятку. Не верьте! В 99 случаях из 100 это звонят мошенники. Не предпринимайте никаких действий, не проверив информацию! Имейте ввиду, что аферисты – отличные актеры и психологи, они очень хорошо умеют моделировать тембр, интонацию, дополнительно ссылаясь на плохое качество связи. Так что разговаривая якобы со знакомым, попавшим в беду, обязательно задавайте контрольные вопросы. Например, как называется фильм, который вы недавно смотрели, или какую книгу вы обсуждали.

Куда можно обратиться за помощью, если вы попались на уловки мобильных мошенников? Борьбой с преступлениями в сфере высоких технологий занимается специально созданное для этих целей Управление «К», входящее в структуру МВД РФ. В отношении лиц, совершающих преступные действия в отношении пользователей мобильной связи может быть применено наказание, предусмотренное статьями 159 «Мошенничество» и 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием» Уголовного кодекса РФ.

Материал подготовила главный специалист-эксперт территориального отдела Управления Роспотребнадзора по Тверской области в Бежецком районе Новикова Г.В.