РОССИЙСКАЯ ФЕДЕРАЦИЯ
АДМИНИСТРАЦИЯ БЕЛОВСКОГО РАЙОНА
КУРСКОЙ ОБЛАСТИ

ПРИЛОЖЕНИЕ № 11
К ПЕРИОДИЧЕСКОМУ ПЕЧАТНОМУ ИЗДАНИЮ - БЮЛЛЕТЕНЬ «БЕЛАЯ»
ОТ 6 МАЯ 2024 ГОДА

Официальное периодическое печатное издание, предназначенное для опубликования

муниципальных правовых актов, обсуждения проектов муниципальных правовых актов,
обсуждения проектов муниципальных правовых актов по вопросам местного значения, доведения до сведений жителей района официальной информации о социально-экономическом и культурном развитии района, о развитии его общественной инфраструктуры и иной официальной информации

Прокуратура Беловского района разъясняет

Мошенничество в сети Интернет: как не стать жертвой

Сотовая телефонная связь, а также интернет-телефония являются одними из наиболее динамично развивающихся видов беспроводной персональной связи. В этой связи большими темпами увеличивается количество преступлений в данной сфере. Преступления зачастую совершаются организованными преступными группами, деятельность многих из них носит транснациональный характер. Среди известных на сегодняшний день преступлений, совершаемых в сети Интернет, особую опасность представляет интернет-мошенничество.

Анонимность, которую предоставляет своим пользователям сеть Интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами делает Интернет наиболее удобным инструментом для мошеннических действий.

Рост числа интернет-магазинов, создание систем предоставления банковских услуг посредством глобальной сети, развитие платёжных систем способствует тому, что всё большее число людей доверяют безналичным расчётам, забывая о том, что даже в виртуальных экономиках действуют криминальные схемы.

В связи с этим для обеспечения своей финансовой безопасности и защиты своих денежных средств необходимо знать наиболее распространенные механизмы, которые используют мошенники, и средства защиты от них.

Основными способами хищения денежных средств с применением информационно-телекоммуникационных технологий являются:

1. Создание «фишинговых» сайтов, т.е. сайтов, содержащих недостоверную информацию о продаже товаров, оказании услуг, высокодоходной инвестиционной деятельности и т.п.

Зачастую такие сайты внешне похожи на официальные интернет-ресурсы (маркетплейсы, сайты объявлений о товарах и услугах, биржи и др.)

Способы обмана различны: товар, за который вы заплатили, просто не отправляют в ваш адрес; вам присылают ссылку на интернет-страницу для ввода данных своей карты, на которую должны поступить деньги за продаваемый вами товар, а после ввода этих данных средства, напротив, списываются с вашей карты; вам предлагают разместить деньги на «инвестиционном» или «биржевом» счете, и каждый день они увеличиваются (иногда в разы), принося вам небывалый «доход», однако любая попытка вывести деньги с этого счета обратно на свою карту будет безуспешной.

Рекомендация: покупайте и продавайте товары только через официальные сайты; не переходите по ссылкам, которые присылает неизвестный вам продавец (покупатель), не вводите данные своих счетов и банковских карт, а также конфиденциальную информацию по ним; не переводите денежные средства на указанные «инвестиционные» и «биржевые» счета, если не имеете достоверной информации о их легальности.

2. Сообщение ложных сведений правового и иного характера (экстремальная ситуация с близким человеком).

Наиболее распространенный способ такого мошенничества – сообщение о проблемах у близких родственников и знакомых (сбил человека в ДТП, нужны деньги для решения вопроса с потерпевшим и правоохранительными органами; требуется дорогостоящее лечение; срочно необходимы денежные средства на иные неотложные цели)

Рекомендация: самостоятельно перепроверяйте доведенную до вас информацию. Даже если позвонившее вам лицо «передало» трубку вашему родственнику (знакомому), в силу психологического эффекта неожиданности вы не сможете определить, с кем разговариваете на самом деле. Прервите разговор и сами перезвоните близкому вам человеку, якобы попавшему в беду. Бывали случаи, когда он находился в соседней комнате, а потерпевший, находясь в стрессовом состоянии, в этот момент передавал деньги мошенникам.

Этот же совет применим в ситуации, когда просьба о финансовой помощи размещена на странице вашего знакомого в сети Интернет. Чаще всего такая страница оказывается взломана злоумышленниками.

3. Социальная инженерия, т.е. конструирование ситуаций, когда человек становится марионеткой в руках злоумышленников и выполняет различные их команды. Здесь также используется эффект неожиданности, а потерпевшему не дают времени на то, чтобы прийти в себя и действовать разумно.

Как правило, в ходе телефонного разговора (как обычного, так и осуществляемого в мессенджерах «Ватсап», «Телеграмм» и др.) неизвестные, представившись следователем, прокурором, оперативным работником МВД или ФСБ, служащим банковской организации, сообщают потенциальной жертве, что мошенники прямо сейчас пытаются перевести с банковского счета принадлежащие ей денежные средства либо оформить на ее имя кредит. Чтобы не допустить этого, необходимо перевести имеющиеся на банковском счете деньги на «безопасный» счет, либо самостоятельно оформить кредит (как в отделении банка, так и дистанционно, в онлайн-приложении), а полученные от банка средства опять-таки перевести на указанный счет. Зачастую звонку мошенников

предшествуют сообщения в мессенджерах якобы от руководителей потерпевшего с указанием ответить на телефонный звонок и следовать полученным инструкциям. К сожалению, большинство из обманутых граждан не решается выяснить у своего начальника достоверность и легитимность такого приказа и идет на поводу у злоумышленников, переводя на их счета миллионы рублей.

Рекомендация: не вступайте в диалог с позвонившим вам лицом, какую бы должность он ни называл и какими бы сведениями о вас ни располагал. Незамедлительно прекращайте разговор, перезванивайте (а лучше - лично являйтесь) в органы прокуратуры, МВД, ФСБ, Следственного комитета России, в банковские учреждения для перепроверки информации. Не сообщайте неизвестному вам собеседнику никакие персональные данные ни о себе, ни о своих банковских продуктах (в т.ч. картах, счетах и т.п.) Не называйте и не пересылайте пинкоды, пароли и другие цифровые и буквенные обозначения, известные вам либо поступившие на ваш телефон. Наконец, не бойтесь лично выяснять у своих руководителей, действительно ли они давали указание о необходимости сотрудничества с тем или иным должностным лицом и выполнения его инструкций.

Помните, что смелость, рассудительность и холодная голова – как раз то, чего от вас не ждут мошенники, что способно сберечь ваши деньги и не дать вам попасть в многомилионную кабалу.

Учредитель: Представительное Собрание Беловского района Курской области,
Сл.Белая, Советская площадь ,1 т. 2-12-08
Тираж 100 экз., бесплатно.
Главный редактор Ярыгин А.М.
Ответственный за выпуск ПЛОХИХ В.В.