**Предупрежден о кибермошенничестве– значит вооружен!**

В последнее время жертвами кибермошенников все чаще становятся люди, которые излишне доверяют информационным технологиям, не очень понимая, как эти технологии работают. Ранее самым привлекательным контингентом для злоумышленников были пожилые граждане.

«Предупрежден– значит,вооружен», гласит народная мудрость. Чтобы уберечь деньгинаших читателей от кибермошенников, мы расскажем о последних хитростях злоумышленников и о способах борьбы с ними.

**Вредоносное письмо**

Пожалуй, практически каждый получал электронное письмо неизвестно откуда с предложением выиграть миллион долларов, помочь начинающему бизнесмену или маленькой стране где-нибудь в Африке.Такие сомнительныепредложения наши здравомыслящие земляки наверняка выбрасывают в корзину.Но время от времени на е‑mail приходят письма вроде бы от серьезного отправителя,которым волей-неволей веришь. Например,могут сообщить,что оператор вашей мобильной связи вводит новую тарифную сетку,с которойпредлагают срочно ознакомиться.Откроешь такое письмо с вложением,не ожидая подвоха, ‒и заразишь свой компьютер вирусом, который умеет воровать чужие деньги.

По данным последнего отчета Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ) Банка России к подобныммошенническим письмам массовой рассылки часто прикладывается вложение-вирус или ссылка на скачивание вируса. Открыл приложение к письму – и на компьютер сами собой устанавливаются различные вредоносные программы, которые воруют пароли, персональные данные, шифруют файлы на жестком диске компьютера и требуют деньги за их расшифровку. «Не следует открывать письма,полученные из ненадежных источников или от подозрительных отправителей. Нельзя проходить по ссылкам в подобных письмах. Если вы хотите установить какую-то программу – нужно скачать ее у лицензированного распространителя», – поясняет управляющий Отделением Белгород ГУ Банка России по Центральному федеральному округуБеленко Андрей Николаевич.

Конечно, поможет установка и регулярное обновление антивирусного программного обеспечения, а также своевременное добавление подозрительных адресатов в список нежелательных отправителей.

**Сплошная «липа»**

Специалисты ФинЦЕРТа рассказывают о таком распространенном способе обмана граждан,как создание «липовых» сайтов банков, страховых компаний, сервисов переводов, сайтов покупки билетов. Никаких реальных услуг они не предоставляют,а только обирают попавших на такие лжестраницы клиентов: у кого украдут данные банковской карты или паспорта, а у кого – и настоящие деньги, переведенные за билет или за оформление кредита. Среди«подставных» сайтов, созданных мошенниками, например,бывают такие,которыезавлекают: «Проверьте, скомпрометирована ли ваша карта!». Человеку предлагается ввести данные его банковской карты, а потом пришедший якобы от банка пароль. Такие сайты-воры созданыдля перехвата ваших данных.

Банк России работает над закрытием сайтов, через которые мошенники вымогают данные и крадут деньги. Так, с января по сентябрь 2017 года ФинЦЕРТ отправил информацию о 481 домене различной мошеннической тематики, владельцев которых предлагалось лишить прав на домен. По данным Банка России, в среднем каждыйкалендарный месяц закрытию подлежит около 50 доменов, находящихся в различных зонах. Наибольшее количество заблокированных доменов приходится на сферу переводов, осуществляемых физическими лицами с карты на карту. На сферу страховых компаний приходится 45 закрытых доменов, на лжебанки– 44, на финансовые пирамиды – 39.Сложность с закрытием вех «неправильных» сайтов состоит в том, что очень многие кибермошенники находятся не в России, а скрываются в других юрисдикциях. Поэтому есть над чем работать.

**Атака на банкомат**

Эксперты мегарегулятора отмечают, что впоследнее время участились атакизлоумышленников на банкоматы: преступники научились управлять ими удаленно. Специальная программа способна найти сервер обновления банкомата и установить контроль над целой сетью устройств. Дальше киберворам остается лишь отправить к банкоматам специальных людей, чтобы они по команде оператора получили наличные.

Существуют группы злоумышленников,которые ставят на банкоматы специальные устройства, позволяющие похитить данные банковской карты пользователя, записанные на магнитную ленту и ее PIN-код. «Выбирайте банкоматы, установленные в хорошо освещенных помещениях. Если вы обнаруживаетена конкретном банкомате подозрительные«накладки», то лучше поискать другой», –отмечаетАндрей Николаевич Беленко.

С 2015 года все банки обязаны выпускать карты только с чипом, ониобслуживаются по технологии 3D Secure– то есть операция сденьгамипроходит только после дополнительного подтверждения с помощью одноразового пароля, отправленного в СМС. Технически перехватитьтакой одноразовый пароль ипохититьсредстваочень сложно. Поэтомумошенникисталимаксимальноактивноиспользоватьметодытакназываемойсоциальной инженериииманипулировать поведением человека с использованием психологических навыков.

**«Социальные инженеры»**

По оценкам аналитиков компании Zecurion, в прошлом году мошенники с помощью социальной инженерии похитили с банковских карт россиян около 650 млн рублей, а в 2017 году ущерб может увеличиться до 750 млн рублей. «Задача любого мошенника,использующегометоды «социальной инженерии» ‒ войти в доверие к своей жертвеизаставить ее выдатьличнуюинформациюили проделать какие-то манипуляции, которые позволят имукрастьвашиденьги», ‒уточняет управляющий Отделением Белгород ГУ Банка России по Центральному федеральному Беленко А.Н..

Например,на мобильный может прийти сообщение, что карта заблокирована, а для разблокировки нужно позвонить по указанному номеру. Стоитперезвонить – излоумышленник на другом конце провода так вас заговорит,что вынудит сообщить коды и пароли от карты,а то ипойти к банкомату якобы для разблокировки. Результат один – жертва сама переводит деньги мошенникам. Что делать? Ни в коем случае не звонить по номеру телефона, указанному в СМС, а пользоваться только номером на обратной стороне карты – уж это точно номер банка, а не киберворов.

С помощью социальной инженерии мошенники пытаются узнатьреквизиты, достаточные для совершения перевода с карты на карту: номер карты, срок ее действия, CVV-код (три цифры собратной стороны банковской карты). Важно помнить, что представители банка никогда – ни по телефону, ни в переписке – не спрашивают полные данные карт, одноразовые пароли, пин-коды. Для консультации им достаточно имени и четырех последних цифр карты.

Поскольку кибермошенники непрерывно придумывают что-то новенькое, нам с вами следует всегда быть настороже,не забывая про здравый смысл.