**Как не попасть на удочку кибермошенников**

В ситуации стремительного перехода информации в цифровую форму каждому необходимо соблюдать правила кибербезопасности. За последние годы число преступлений, совершаемых в сфере информации и телекоммуникаций выросли в несколько раз. В топе 5 основных глобальных рисков с точки зрения вероятности на
2018 год значатся кибератаки, кража данных и мошенничество.

Что такое кибербезопасность?

Это основа нашей безопасности в мире информационных технологий, обеспечения конфиденциальности, целостности и доступности данных.

Кибермошенничество набирает обороты. Преступники списывают деньги со счета человека без его ведома, обещают огромные проценты по вкладам, продают поддельные страховые полисы. Жертвой может стать любой.

Банк России старается работать на опережение. Создан и эффективно работает Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ). С его помощью блокируются фишинговые сайты и ресурсы, с помощью которых распространяется вредоносное программное обеспечение. Фишинг (от англ. «рыбалка») – это разновидность кибермошенничества. Такие сайты имитируют добросовестные банки, микрофинансовые организации, кредитные потребительские кооперативы, страховые организации. Цель злоумышленников – получить доступ к личным данным пользователей. Например, к логинам и паролям, к данным банковских карточек. Делается это через письма со ссылкой на сайт, который представляет собой копию настоящего. Пользователь не замечает, что сайт поддельный, переходит по ссылке и вводит на этом сайте-клоне свои личные данные, например, данные своей карты, либо запускает программу, которая сама ищет пароли на вашем персональном устройстве.

Впрочем, человек и сам может наткнуться на нелегальных кредиторов, когда ищет в интернете, где бы занять или куда под наибольший процент вложить деньги, и натыкается на фишинговые сайты, в том числе коммерческих банков с сервисами кредит-онлайн. В этом случае мошенники расставляют ловушку следующим образом. Расчет мошенников прост: не все люди внимательно смотрят на адресную строку браузера, и не все понимают, что сайт только похож на привычный сайт, на самом деле являясь совершенно другой страницей. Человек без колебаний заполняет заявку на кредит, порой раскрывая данные своей банковской карты, ‒ а в конце онлайн-цепочки остается и без заемных, и без собственных денег.

Сегодня преступники получают информацию о конкретном человеке и через соцсети. Например, вы упомянули, как зовут ребенка или любимую собачку? Дали как минимум два варианта пароля, которые часто используют граждане. Обозначили, что мечтаете о поездке на море? Вам через некоторое время могут позвонить или прислать сообщение, что вы якобы выиграли тур, нужно лишь перечислить «стартовый взнос». Кибермошенники стали вовлекать в свои махинации даже детей. Преступники звонят по случайным номерам. Если трубку взял ребенок, ему говорят, что он выиграл крупный приз, и просят продиктовать номер банковской карты родителей и код с обратной стороны. Но взрослым при этом ничего не говорить - мол, сюрприз будет.

Чтобы не стать жертвой мошеннических сайтов, соблюдайте правила кибергигиены:

- в случае поступления на телефон, либо на адрес электронной почты сообщения от неизвестного пользователя, содержащего какие-либо файлы либо ссылки на интернет-адреса, не открывайте данные файлы и не переходите на указанные ссылки;

- при входе на различные сайты организаций внимательно изучите название сайта и его содержание, убедитесь, что это не сайт-двойник, не вводите свои персональные данные и данные банковских карт на сайтах, вызывающих подозрения;

- не соглашайтесь на скачивание файлов из неизвестных источников и с неизвестных сайтов, не открывайте скачанные автоматически файлы;

- используйте на устройствах антивирусные средства с актуальными сигнатурными базами;

- не следует совершать покупки в сомнительных интернет-магазинах и помните о том, что все официальные интернет магазины предлагают покупателям различные системы оплаты их товара, не только через сеть Интернет.

21.03.2018

Отделение по Костромской области

Главного управления Банка России

по Центральному федеральному округу

Телефон: (4942) 62-71-63

34media@cbr.ru

