Кибербезопасность:

сохранность информации в ваших руках

Александр НАСОНОВ,
президент Объединения структур безопасности «Тауэр»

В XXI веке – веке информации – люди все активнее используют электронные устройства: для переговоров – сотовые телефоны, для проведения платежей по банковским картам – банкоматы и терминалы, для совершения покупок и продаж, а также для виртуального общения – Интернет… В процессе пользования такими, без сомнения, полезными современными механизмами многие напрочь забывают о риске, связанном с сохранностью их данных. О кибербезопасности – новом понятии, вошедшем в нашу жизнь, мы говорим с доктором делового администрирования, президентом Объединения структур безопасности «Тауэр», руководителем комитета по безопасности предпринимательской деятельности Торгово-промышленной палаты Ивановской области, официальным представителем МААК в нашем регионе Александром НАСОНОВЫМ.

? Александр Вячеславович, сегодня многие получают зарплату по банковским картам, да и просто используют их в качестве удобного платежного средства. Насколько проблема кибермошенничества актуальна для держателей таких карт?

– Весьма актуальна. На слуху недавняя история с одним из банков, в которой фигурируют шокирующие цифры: в результате действий киберпреступников со счетов граждан незаконно были списаны порядка 2 млрд рублей.

Как правило, люди, открывая пришедшую на мобильный телефон смс от неизвестного адресата, сами того не подозревая, запускают вирус – троян. В результате действия трояна преступникам становится доступна вся информация о ваших личных счетах, паролях и прочие данные. Завладев ими, мошенники с легкостью снимают со счетов граждан денежки, иногда небольшими суммами, чтобы было не так заметно, параллельно с этим блокируя смс-уведомления на ваш телефон о списании средств. Оповещения вам на телефон под действием хакерской программы просто не приходят, и вы до поры до времени знать не знаете о проблеме. Мой совет: смс с незнакомых номеров просто удаляйте, даже не открывая.

Обналичивать деньги с карты стоит лишь в том случае, когда поблизости нет веб-камер и посторонних людей, которые могут увидеть ваш пин-код. Мошеннику будет несложно, прицепив к банкомату незаметное устройство для считывания пин-кода, сделать в дальнейшем магнитный клон карты и снять деньги с вашего счета.

Также нередки случаи, когда пользователи Интернета оплачивают различные приложения при помощи банковских карт, не подозревая, что эти сайты небезопасны. В итоге деньги полностью списываются, и люди остаются на бобах... Во всех описанных ситуациях нельзя забывать о бдительности.

? Насколько преуспели мошенники в воровстве информации, используя мобильные телефоны, которые сегодня есть даже у детей?

– Увы, и здесь ситуация нерадостная. Зная ID телефона (его идентификационный номер), преступник незаконным путем без труда добудет интересующую его информацию о гражданине. С помощью идентификационного номера в телефон можно закачать программы-шпионы, которые позволят преступнику дистанционно отслеживать и читать на своем компьютере всю информацию, которая будет в телефоне кибержертвы. Без ведома владельца телефона мошенники могут записывать видео, звук...

Чем проще по своим техническим характеристикам телефон, чем ниже его стоимость и проще функционал, тем легче преступнику использовать его в своих целях. В более дорогих устройствах, где установлены антивирусные программы для мобильных телефонов, проблема утечки информации менее актуальна, но и они не застрахованы на 100% от потери данных.

Как защитить себя от этого вида мошенничества? Все просто и вместе с тем очень важно: не покупайте телефон с рук, не передавайте его сторонним лицам даже на время, не разрешайте звонить с вашего телефона незнакомым людям и не оставляйте его без присмотра.

? Ни для кого не секрет, что всех нас сегодня затягивают сети – социальные. Чем стоит руководствоваться пользователям при общении в виртуальном пространстве, чтобы не попасть на удочку мошенников из-за собственной открытости и излишней доверчивости?

– Да, сейчас люди активно публикуют на своих страничках в соцсетях подробности личной жизни, домашний адрес, фотографии квартиры, информацию о предстоящих поездках. Для многих преступников подобные публикации становятся наводками, так как по фотографиям они могут оценить, есть ли в доме предметы роскоши, а по публикациям узнать, что на определенное время квартира будет пустовать. Кроме того, в дальнейшем информация, размещенная в Интернете, может повредить карьере или личной жизни, вот почему так важно, чтобы люди с ответственностью подходили к публикациям данных о себе. Пароли следует выбирать усложненные, периодически их менять.

Из всего сказанного стоит вынести главное правило: человек сам способен как спровоцировать негативную ситуацию, при которой излишняя открытость будет обращена против него самого, так и обезопасить себя вовремя предпринятыми действиями. Если перефразировать поговорку «болтун – находка для шпиона» на современный лад, то в нынешних условиях она приобретет более актуальное звучание: «активный пользователь гаджетов – находка для кибермошенников». Знаете, это как ситуация с мечом – он может как защитить, так и навредить. И пользу принести, и вред. Стоит лишь научиться обращаться с «оружием» - информацией.