Безопасность в сети и жизни

► Как уберечь себя от кибератак, что такое цифровая гигиена и почему жертвой мошенников может стать любой из нас, разбирался корреспондент «НБ».

Может коснуться каждого

Неделю назад мне позвонили из банка. Молодой человек спокойно представился работником службы безопасности, назвал внутренний номер сотрудника, не вызвав подозрений. Общались не меньше десяти минут. Со стороны всё выглядело прилично и даже профессионально: «сотрудник банка» сыпал терминами, объяснял важность своего звонка и ни разу не заикнулся о паролях, номерах карт и других данных, так необходимых мошенникам. Ровно до одного момента.

Подозрения появились, когда он стал рассказывать, почему именно сейчас мои деньги находятся в большой опасности, а сам я могу попасть под уголовную ответственность, если мы не решим вопрос сиюминутно. И тут меня осенило: если пытаются вывести на эмоции, вселить чувство страха - значит, что-то нечисто. Вежливо попросив перезвонить попозже, я столкнулся с непробиваемой решимостью человека на том конце провода - ещё один сигнал! «Сотрудник» настойчиво просил не бросать трубку, апеллировал к серьёзности положения и прямым текстом призывал как можно скорее решить вопрос. Это типичное поведение мошенника: не отпускать «разогретую» жертву, чтобы она не остыла.

Молодой человек не давал никакого пути отхода - пришлось просто положить трубку. Ситуация, мягко сказать, тревожная, поэтому я сразу полез в приложение банка, чтобы проверить, на месте ли мои кровные. Не тут-то было! Следом поступил звонок с другого номера - на проводе тот же «сотрудник». Это был последний гвоздь в крышку мошеннического гроба - человек не справился с эмоциями и выдал себя с головой. Однако моя бдительность оказалась даже излишней: как только я всё же зашёл в приложение, оно само объявило мне, что звонили мошенники и чтобы я ни в коем случае не переводил никому деньги и не сообщал данные. Я всегда думал, что такие истории происходят «где-то не здесь и не с нами», пока лично не убедился в силе внушения недобросовестных людей.

Что и говорить: по данным Центробанка, в первом квартале 2022 года мошенники обманули россиян 258 097 раз, а жертвы киберпреступников расстались в общей сложности с 3,3 млрд рублей - на полмиллиарда больше, чем в прошлом году. Мы стали слишком доверчивыми или мошенники чересчур находчивыми? Поиск ответов привёл меня на лекцию «Кибербезопасность в эпоху Big Data» кандидата технических наук и доцента БГТУ им. В.Г. Шухова Игоря Гвоздевского. Лекция проходила 15 сентября в белгородском Центре молодёжных инициатив, вход был бесплатным, так что узнать о преступлениях в цифровой сфере и способах их недопущения мог каждый.

Что за Big Data?

В контексте этой встречи термин «Big Data» (с английского - большие данные) использовался как описание положения, когда основная информация о нас, наши личные данные и действия отображаются и хранятся в интернете. По мнению Игоря Гвоздевского, это несёт как положительные изменения в обществе, так и представляет существенную опасность для него.

- Смартфон - это новая концепция, которая очень хорошо зашла на рынок. С одной стороны, это помогло открыть новые просторы неизведанного, вовлечь людей в новые технологии, в изучение новых стандартов, - начал свою лекцию он. - С другой стороны, это сподвигло на развитие теневой стороны: выросло влияние вредоносных элементов на нашу обычную жизнь. Сейчас телефон - это часть нашей жизни, и если в обычном пространстве мы можем её как-то защитить, например, запереть дверь квартиры, то в электронных устройствах технологии защиты оставляли широкие возможности для злоумышленников.

Говоря об имеющемся объёме данных, Игорь привёл примеры, насколько много уже сейчас информации производится и содержится на серверах. По словам лектора, ежеминутно в Twitter публикуется 456 тыс. постов, за это же время в Google поступает 3,6 млн. поисковых запросов, а в Facebook* ежедневно загружается 300 млн. фотографий.

О чём пишут в лицензионных соглашениях?

Чуть позже лектор коснулся примеров того, как просто заполучить наши данные, не нарушая закон. Оказывается, мы и сами нередко даём на это согласие, даже об этом не подозревая.

- Давайте честно признаем: мало кто из нас читал лицензионное соглашение, которое предваряет установку того же самого мобильного приложения «ВКонтакте» или Facebook*, - говорит Игорь Гвоздевский. - Если вы внимательно ознакомитесь с этими документами, то там есть явный намёк на то, что какими-то данными вам придётся пожертвовать во благо развития человечества. Естественно не только человечества, но и на пользу коммерческим интересам этих компаний.

Мало того, кто-то готов добровольно впустить в свою частную жизнь корпорации, получая за это деньги.

- В США был проект, в рамках которого пользователи получали ежемесячно по 20 долларов за то, что их данные анализировались компаниями. Вы готовы за 1,5 тысячи в месяц дать кому-нибудь свой телефон, чтобы там всё посмотрели? - с улыбкой поинтересовался лектор.

Чем опасны утечки информации?

- На сегодняшний день данные, которые так или иначе циркулируют в социальных сетях, являются лакомым куском, потому что могут использоваться в многоступенчатых атаках, реализации угроз, шантаже, вымогательстве и других воздействиях для получения выгод, - объясняет Гвоздевский.

Даже если такая невинная информация, как номер телефона, попадёт в руки злоумышленников, это уже многократно повышает риск быть обманутым.

- Мошеннические схемы могут быть по-разному реализованы, - рассказывает Игорь. - Звонок о крупном выигрыше в лотерею или тот же самый обман через сообщение СМС, когда вам шлют информацию о том, что ваш родственник попал в аварию. Большая часть таких угроз связана именно с человеческой психологией и реализацией поведенческих мотивов. Это социальная инженерия: обычный разговор по душам, в ходе которого к вам входят в доверие, а дальше вы сами помогаете злоумышленникам получать доступ к вашим деньгам или персональным данным.

Как защитить свои данные?

В качестве мер противодействия мошенникам Игорь Гвоздевский поделился советами по безопасности в сети и жизни. Первое и основное - не делать поспешных решений!

- В первую очередь перед тем, как что-то сделать, нужно задать себе вопрос: «Правильно ли я поступаю?». Важно не поддаваться эмоциям. Вы должны дать себе возможность принять правильное решение. Если вам поступил звонок, с вас требуют деньги или предлагают какую-то услугу, сначала подумайте о том, что происходит, попросите дать вам время для принятия решений. Когда эмоции утихнут, вы уже с трезвой головой будете противодействовать злоумышленникам, - советует Гвоздевский.

Лектор назвал ещё ряд правил и инструментов, которыми стоит руководствоваться, чтобы не быть обманутыми:

- использовать лицензионные программы крупных разработчиков;
- разделять рабочее и личное пространства (иметь несколько телефонов, электронных почт для разных целей);
- подключать двухфакторную аутентификацию, придумывать надёжные пароли или пользоваться генератором паролей;
- не переходить по подозрительным ссылкам;
- не давать детям смартфон или компьютер, не объяснив, как им можно пользоваться, а лучше всего - настроить детский режим (безопасный интернет).

В конце лекции Игорь Гвоздевский ответил на вопросы слушателей. Мы узнали, каким антивирусом стоит пользоваться. Ответ озадачил и даже обрадовал:

- Большинство антивирусных продуктов даже в базовой версии выполняют тот функционал, для которого предназначены. Они решают 80-90 % задач, которые встают перед пользователями. Остальное - продуктовая маркетинговая стратегия. В целом, базовая защита от вирусов, которая предоставляется в пакете операционных систем, и даже популярные бесплатные аналоги решают большинство проблем, - отметил он.

Отвечая на вопросы, специалист подчеркнул, что в условиях повсеместного импортозамещения нам не стоит беспокоиться по поводу отсутствия нужных сервисов. Многие из них даже более доступны, чем зарубежные аналоги.

- Наша IT-отрасль, кто бы что ни говорил, очень развита. Даже на текущий момент многие отечественные продукты достаточно эффективны. Много бесплатных вещей, которые можно попробовать прямо сейчас.

Никита МИГУЛИН
ФОТО АВТОРА

* - *принадлежит группе компаний Meta, признанной в России экстремистской организацией.*