**11 правил сетевой безопасности: как защититься от кибермошенников**

Мы привыкли работать и практически жить в интернете, и совершенно забываем о том, что защищать свое онлайн-пространство надо точно так же, как свой дом

Понятно, что хакеров прежде всего интересуют финансовые ресурсы и информация. Информация о наших деньгах – самое важное для киберпреступников. Но как они ее находят, где видят? Человеку, не имеющему специальной подготовки, не имеет смысла приводить способы разработки личного счета «клиента». Но есть и хорошие новости. Небогатые люди хакеров мало интересуют.

Вот ярчайшая деталь: специалисты по борьбе с киберпреступностью рассказали, что во время расследований одного из эпизодов деятельности хакерской группировки, занимающейся «вскрытием» частных счетов, выяснилось, что данные на тех людей, у которых на счету было меньше 50 тысяч рублей, хакеры откладывали в специальную папку под названием «бомжи».

Илья Сачков, президент компании Group-IB , занимающейся расследованием компьютерных преступлений, утверждает – если вы знаете правила технической самозащиты, вы будете в безопасности. Компания уже десять лет разрабатывает специальные памятки, в которых рассказывает, что делать, чтобы кибермошенники не воспользовались вашей информацией. Но распространение в обществе этих знаний идет чрезвычайно медленно.

«Мы считаем, что в школе часть уроков ОБЖ должна быть посвящена защите от киберпреступности. Потому что противотанковая граната сегодня более редкий способ вреда, чем киберпреступность», – говорит Илья Сачков.

Рекомендуем вам использовать 11 простых правил самозащиты от специалистов по кибербезопасности компании Group-IB:

 К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

Храните номер карточки и ПИН–коды в тайне. Запомните и сотрите/заклейте CVC-код

Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

 Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма.

Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах.

 Проверяйте запросы персональных данных из каких-либо деловых и финансовых структур. Лучше обратиться в эти структуры по контактам, указанным на официальном сайте, а не в электронном письме.

Насторожитесь, если кроме вас в электронном сообщении указаны другие адресаты. Крайне маловероятно, чтобы при общении с клиентом по поводу личных учетных данных банк ставил кого-то в копию.

Насторожитесь, если от вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у вас ощущение тревоги, чтобы заставить вас действовать быстро и неосмотрительно.

Для чего это нужно делать? Какие опасности нас подстерегают?

Основная цель киберпреступников – интернет-банки. Количество атак на них, по данным правоохранительных органов, – растет стремительно, прирост от 80 до 200 процентов ежегодно. Интернет-преступления удобны: можно украсть миллион, не вставая с кресла. Границы не важны – опять же сидя на своем диване вы в состоянии совершить преступление одновременно в ста странах. Современные законы не успевают за действиями хакеров, в итоге те часто уходят от возмездия.

А еще компьютерные преступники не вызывают у общества негативных эмоций – и этот вид преступлений оказывается общественно безнаказанным. Надо признать: у хакеров высокий уровень IQ, не так-то просто вскрывать защищенные данные и воровать информацию. Поэтому этот вид противоправной деятельности в определенной степени романтизирован. Киберпреступниками часто оказываются совсем молодые люди. Следователи говорят, что часто родители арестованных хакеров вообще не знали, чем занимается их ребенок. Думали, например, что он делает сайт интернет-магазина, и так далее. Так что наша собственная беззащитность может начинаться с нашей же собственной семьи – с того, чем занимается близкий человек в соседней комнате.

Но кибермошенников могут интересовать не только деньги – но и ваши личные данные.

Вы можете стать жертвой бытового «наезда» – в результате скажем, рабочего или частного конфликта – и в этом случае, если ваши данные не защищены, вы можете потерять свой архив, рабочие разработки – или, напротив того, ваши приватные записи или снимки могут стать достоянием гласности. Последнее особенно важно для людей публичных. Впрочем, каждый из нас дорожит своей репутаций и правом тайны личной переписки.

Безопасная электронная почта

Чаще всего мы ведем документацию с помощью своей электронной почты: пересылаем документы, ведем деловую переписку. На почту мы получаем подтверждения о наших заказах, покупках. Как защитить свою электронную почту? Одно из простых правил: мухи отдельно, котлеты отдельно. Важно понимать, для чего именно вы используете свой почтовый ящик.

«Стоит помнить, что есть платные сервисы для почты, есть бесплатные, а есть корпоративные. Степень защиты предоставляет администратор сервера. Для корпоративной почты есть подробные требования, в них написано, что можно, а что нельзя делать сотруднику соответствующего предприятия. Платных сервисов «обычные» пользователи избегают, не хотят тратиться, но если нужна защита почты, надо читать пользовательское соглашение и следовать ему.

А уж тем более, если вы выбираете бесплатную почту. У нас вообще нет культуры пользовательских соглашений, к сожалению», рассказал корреспонденту «Милосердия.ru» Михаил Якушев, один из ведущих российских экспертов по киберправу, вице-президент корпорации ICANN по России и Восточной Европе.

Что касается интернет-грамотности детей, то, советует Михаил Якушев, родители должны объяснять детям, что если ты хочешь получить новую услугу – ресурс, адрес – сначала изучи, на каких условиях тебя будет обслуживать оператор, а при каких обстоятельствах тебя могут отключить. Тем более, что именно родитель отвечает за действия детей и в первую очередь прочесть все условия и изучить требования должен именно взрослый. Важно также, чтобы информация с почты никуда не передавалась, не вскрывалась и не читалась.

«Каждая почта должна использоваться для определенных целей. Допустим, через корпоративную почту не надо осуществлять покупки в интернет-магазинах для личного потребления. Это может отслеживаться и это может куда-то попасть. Для связи с электронными магазинами, для покупки личных авиабилетов корпоративную почту тоже не стоит использовать – в ней останется информация о ваших финансах.

Лучше переписываться на такие темы там, где будет повышенная защита вашей информации, – отмечает эксперт. – Вообще, стоит помнить, что бесплатная почта не может гарантировать конфиденциальность. Если вы пересылаете с бесплатного почтового ящика данные паспортов, банковских карт и так далее – это может быть опасным».

Есть определённые правила работы со спамом. «Не нужно проходить по неизвестным ссылкам, не нужно открывать ссылки от незнакомцев, а если знакомый присылает странный файл с подозрительным расширением, лучше сначала перезвонить ему и убедиться, что это прислал вам действительно он, проверить, что ждет вас по ссылке, прежде чем открывать ее», – советует Михаил Якушев.

А можно ли выбрать самого безопасного почтового оператора? Трудно сказать, какой почтовый оператор лучший. «В первую очередь, нужно исходить из того, насколько пользовательское соглашение понятно и нравится вам, – поясняет специалист. – Чего от вас хотят, и чего хотите от почтового сервиса вы. Важно убедиться в действующей обратной связи с пользовательской поддержкой почтового сервера. Например, ваш ящик вскрыли, или вы забыли пароль – кто вам будет помогать? Смогут ли восстановить ваши данные? Лучше предварительно позвонить по телефону почтового сервера и убедиться, что он действующий, и что это именно та самая обслуживающая компания».

Опасности открытого пространства

Существует ли более серьезная опасность, если мы пользуемся почтой через телефон? Это неважно, говорят специалисты, – Главное – защита самого почтового трафика.

Однако важно, где именно вы пользуетесь почтой – у себя дома или в публичном пространстве.

 как узнать, проник ли хакер в вашу почту? Какими методами пользуются кибермошенники? «Самые популярные методы известны, и они, к сожалению, достаточно эффективны при невнимательности пользователей. Чаще всего это перехват пароля и логина при авторизации в почте.

Это может происходить, если вы сидите в кафе или в открытом вай-фае, – рассказывает Михаил Якушев. – Ваши данные преступники могут отследить через видеонаблюдение, или через перехватывающий радиосканер. Могут даже с помощью специальных устройств по звуку вычислить, какой пароль вы набрали – клавиши издают при наборе разные звуки. Здесь решение проблемы – лишний раз не заходить на свои аккаунты или почты в общественных местах, внимательно следить, где вы вводите этот пароль. Можно воспользоваться дополнительной защитой – когда вы вводите пароль, и приходит смс-подтверждение по телефону: в этом случае будет непросто вскрыть вашу почту».

Второй способ вскрытия вашей почты, отмечает эксперт, еще более простой и распространенный: вам приходит предложение посмотреть картинку или сайт, а это заражает ваш компьютер или передает вашу личную информацию злоумышленникам. «Это самый дешевый и простой способ. Какой-то процент пользователей попадает на эту хитрость, начинает переходить на хакерские ссылки, разглядывать картинки, читать тексты, – а у них в итоге воруют информацию. Надо уметь отличчать спам и не ходить по спамерским ссылкам».

Еще нужно убедиться, что письмо пришло именно от того отправителя, которого вы знаете, – советует Михаил Якушев. Иногда хакеры присылают письма от известных вам адресантов. Но здесь проверить благонадежность отправления сложнее – нужна техническая проверка.

Как защитить свои деньги в интернете?

Как воруют информацию о банковских картах? С них точно так же считывают информацию. «Визуально или с помощью технических средств ее легко перехватить на банкомате с помощью так называемых скиммеров, – поясняет Михаил Якушев. – Также хакеры по определенному алгоритму могут вычислить, в каком электронном сообщении находится информация о карте, и воруют ее».

Недавно и сам наш эксперт стал жертвой киберпреступников. «Я пользовался одним зарубежным сервисом по покупке авиабилетов, и при покупке и переводе средств, видимо, какие-то данные были перхвачены. Затем мне пришла смс, что с моей карты снята маленькая сумма в 10 долларов – за какое-то обслуживание. Но я заметил это и сразу пошел разбираться в банк. Было оперативно установлено, что сумма была списана сайтом, который незаконно собирает деньги с клиентов. Деньги быстро были возвращены.

Пользователям карт нужно быть внимательными, и следить за любым списанием средств со счета. Правда, когда сайт находится за пределами страны проживания потерпевшего – поймать таких злоумышленников сложно. Еще одна хитрость – если вы делаете платёж в интернете, то используйте ту карту, на которой ровно столько средств, сколько надо, чтобы оплатить покупку, – чтобы злоумышленникам не досталось остального».

Процент возбуждения уголовных дел по подобным случаям небольшой, и достоверной статистики здесь мало. «Злоумышленники действуют чаще за пределами страны, где находится их жертва. То есть наши российские хакеры предпочитают делать атаки на американских владельцев карт, и наоборот, у нас работают европейцы, украинцы, молдаване, и так далее. А когда выясняется, что подозреваемый за границей, полиция разных стран не всегда может скоординировать между собой действия и в итоге привлекать хакеров к ответственности, – рассказывает Михаил Якушев. – Я сам участвовал в таких транснациональных операциях, когда вместе взаимодействуют правоохранители России, Европы, Интерпола, США. Это помогает, и тогда дело можно довести до конца.

Но это чаще происходит с киберпреступностью в США: в небольших странах Европы или Латинской Америки большая степень доверия местным следователям, и они соглашаются, чтобы на их территории расследование проводили американцы, англичане – те специалисты, у кого больший опыт в этом. В некоторых азиатских странах большой процент доверия нашим российским специалистам. А вот сильные игроки друг другу могут и не доверять. Поэтому нелегко наладить такое общемировое взаимодействие следственных органов. Но даже в условиях, не очень хороших с точки зрения политики или дипломатии, на уровне борьбы с кибер-преступностью между странами налаживается диалог. Все понимают, что это общая проблема».

Может ли хакер отключить кардиостимулятор или аппарат ИВЛ?

Насколько опасна киберпреступность в научной и технической сфере? Есть городская легенда, пока не подтвержденная, что хакеры могут войти даже в информационную систему госпиталя и отключить, например, аппарат искусственной вентиляции легких, и в итоге человек умрет. Это уже атаки на инфраструктуру.

Михаил Якушев отмечает, что подобные рассказы о выведении хакерами из строя медицинских аппаратов – пока недоказанная информация, хотя они и леденят душу: ведь это совершенно новый, фантастический способ расправиться с кем-то. Собственно говоря, новый способ бесконтактного убийства. Но вообще, подобные атаки на инфраструктуру вполне возможны и очень опасны.

«Это может касаться и нарушения работы транспорта. Представьте, например, что будет, если нарушить компьютерную систему московского метрополитена? Произойдет коллапс. А если хакеры произведут атаку на авиацию или сферу атомной энергетики? Это очень опасно. И связано с недопущением воздействия злоумышленников на технологические системы, а не на деньги или информационную систему. В условиях, когда к технологиям подключается интернет, это становится все более актуальным. Интернет удобен, но и методы противоправного использования технологии становятся часто применимыми», – говорит Михаил Якушев.

Это самое острое и бесспорное направление сотрудничества между странами и самая опасная проблема. Как можно бороться с киберпреступностью в этих сферах?

«Один из способов – использование надёжных межсетевых экранов, которые не позволяет информации из одной системы несанкционированно попасть в другую информационную систему. Это нечто вроде дверей и окон вашего дома, которые не пускают к вам злоумышленника. Как вы понимаете, трудно представить, что система управления ядерными силами использует открытые для всех интернет-каналы. Конечно, там все сложнее – в этой сфере свои методы построения сети, она не связана с теми IT-технологиями, которые мы используем в быту. Например, это можно сравнить с тем, что вы включаете свет в доме, а сквозь занавески на улицу свет не проходит – не виден. По такой же аналогии строится работа сетей в сложных стратегически важных областях. Но это очень дорого – сделать свои сети непроницаемыми, защититься от атак. Кроме защиты от внешнего проникновения через сеть, здесь так же важно предотвращать утечку информации через технические носители».