Тема киберпреступлений, иначе говоря, преступлений, совершенных с использованием сети «Интернет», сегодня актуальна, как никогда. Все знают. Все об этом говорят, но несмотря ни на что, ежегодно на счета злоумышленников перетекают многомилионные реки денег простых граждан, не позаботившихся о собственной кибербезопасности.

Напомним основные правила поведения в сети «Интернет»:

1. Тщательно контролируйте своё поведение в социальных сетях. Мошенники-виртуозы очень искусны в использовании личной информации, с помощью которой они с лёгкостью могут взломать коды безопасности, и получить доступ к другим учётным записям. За последние несколько лет этот способ кибератаки стал одним из самых распространённых. Речь здесь идет не только и не столько о персональных данных, которые большинство уже научились не афишировать чрезмерно, но даже о фотографиях, переписке, комментариях, из которых часто можно выудить информации куда больше, чем мы думаем.

2. Для сохранности ваших учётных записей ограничьте доступ к внутреннему кругу друзей и близких. Никогда не делитесь личной информацией с новыми интернет-друзьями. Старайтесь не афишировать данные, содержащие даты рождения, адреса электронной почты или имена домашних животных, которые могут использоваться как пароли. Вся эта информация может оказаться весьма полезной для профессионального хакера.

3. Старайтесь минимизировать использование банковских карт онлайн и уж точно никогда не вводите данные своих дебетовых карт на непроверенных сайтах. Пользуясь полученными от Вас же данными, злоумышленники получают таким образом совершать несанкционированные платежи и переводы с карты, которые изымают денежные средства непосредственно с Вашего банковского счёта, и даже если немедленно сообщите о нарушении, на восстановление прежнего баланса потребуется не одна неделя – и это еще если повезет. Не забывайте про функцию оповещения на электронную почту или в виде СМС-текста, что даёт возможность быстрого прерывания несанкционированных действий.

4. Остерегайтесь сообщений подобного рода: «Внимание! Ваш аккаунт был взломан. Вы должны позвонить, чтобы подтвердить свой аккаунт. Отправьте нам сообщение, и мы перезвоним Вам. Сообщите нам пин-код карты и мы остановим утечку денежных средств». Ни под каким предлогом не сообщайте в таком случае свои паспортные данные, данные банковской карты и любые другие сведения о себе, кем бы ни представлялись авторы звонка или сообщения (сотрудники банка, полиции и т.д.). Запомните, если получили сообщение или звонок подобного содержания, лучше всего положить трубку и самостоятельно перезвонить в свой банк, уточнив информацию.

5. Никогда не переходите по гиперссылкам из электронных писем, сообщений в соцсетях и мэссенджерах, даже если на первый взгляд, они выглядят как безобидный контент или отправлены от знакомого вам адресата (в последнем случае не поленитесь уточнить у отправителя, действительно ли именно он отправил Вам эту ссылку и известно ли ему ее происхождение – он ведь тоже мог просто бездумно перейти по непроверенной ссылке). Часто при нажатии ссылки открывается канал для вредоносных программ, которые могут вторгнуться в компьютер или передать вашу личную информацию. Нередко вредоносные программы скрываются до поры до времени, и Вы не узнаете, что скачали ее, пока, например, со счета не пропадут деньги.

6. Не будьте опрометчивы в использовании Wi-Fi соединения. Горячие (общего пользования, например, в кафе) точки Wi-Fi чаще всего небезопасны, так как не кодируют информацию, передаваемую в интернете. Более того, инструменты, которыми пользуются хакеры, позволяют им «заглянуть» в Ваш компьютер и выудить имена пользователей, пароли или другую информацию, предоставляющую доступ к финансовым счетам. Сотовая сеть в этом плане более безопасна.

7. Внимательно проверяйте URL-адреса, на которые переходите, даже если они содержат имена авторитетных учреждений, с которыми вы уже имели дело. Самый распространённый подвох – это комбинация имени законного веб-сайта и подделки. Достаточно лишь одного неверного, лишнего или недостающего символа, чтобы попасть на

сайты-подражатели, которые под внешне законным видом скрывают принадлежность к хакерской деятельности. При этом, даже сам сайт внешне может быть идентичен подлинному, что не должно вводить в заблуждение.

8. Никогда не кликайте на сообщения, присланные на электронную почту и предлагающие обновить персональные данные, если только сами не запрашивали информацию для их смены. Скажем, на электронной почте Вы обнаружили письмо, предлагающее сменить пароль на сайте (даже если посещаете его регулярно), подтвердить регистрацию и т.п., хотя Вы такую информацию не запрашивали и регистрироваться ни на каких сайтах не пытались. Можете быть уверены, что автор письма – кибермошенник, который жаждет выудить у Вас нужную ему информацию, или получить доступ к Вашему ПК.

9. Не используйте одинаковый пароль для разных учётных записей. Выбирайте для паролей необычные символы, цифры и пробелы. Никогда не используйте в качестве паролей комбинации одинаковых символов, даты рождения родных и близких, имена животных, дорогих людей и прочую личную информацию, даже если при этом меняете раскладку клавиатуры. В качестве дополнительной меры предосторожности, заполните вопросы безопасности вымышленными, простыми для запоминания ответами, а не фактами, которые могли бы раскрыть ваши личные данные.

10. Установите на компьютер лицензионное антивирусное и антишпионское программное обеспечение. Убедитесь, что эти программы работают и обновляются автоматически.

11. Устанавливайте на компьютер только лицензионное программное обеспечение, поскольку только оно гарантированно не содержит вредоносных программ и кодов. Программы, скачанные в интернете, снабженные всевозможными «кряками», уже прошли через «заботливые» руки хакера – можете ли Вы быть уверены, что в качестве «бонуса» этот человек не снабдил программу вирусом?

ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРОКУРАТУРА АСТРАХАНСКОЙ ОБЛАСТИ

АХТУБИНСКАЯ ГОРОДСКАЯ ПРОКУРАТУРА

РЕКОМЕНДАЦИИ ПО КИБЕРБЕЗОПАСНОСТИ

= Ахтубинск 2023 =