Что можно и чего нельзя делать в Интернете

Владимир Безмалый

Сегодня мы с вами все чаще и чаще фактически живем в Интернете. И несмотря на то, что большинство людей использует для общения различные приложения (причем все чаще это мобильные приложения), это не означает что правила поведения в Интернете изменились.

Вместе с тем стоит отметить, что как только очередная партия новичков чему-то научится (к сожалению, на своих ошибках), им на смену приходит следующая волна с мыслью «Да чему нас могут научить эти старики!». Ведь, по их мнению, технологии быстро развиваются, а значит преподаватели их ничему научить просто не могут!

Это не так. Ведь взломщики все так же ищут личную информацию, которую могут использовать для доступа к вашей платежной информации, все так же ваши данные можно продать. А уж тем более данные вашей компании! Помните, сколько бы лет ни прошло, мы с вами просто товар! А раз так – учитесь строить вашу же безопасность!

К чему может привести небезопасный серфинг в сети Интернет? В первую очередь вы можете столкнуться с неприятными личными комментариями в сети, с изображениями, которые, оказавшись в Интернет, практически невозможно удалить, с людьми, с которыми вы предпочли бы не иметь ничего общего. Что делать?

Постарайтесь соблюдать определенные правила, чтобы избежать проблем.

Не распространяйте вашу личную информацию

Понимаю, что в век использования социальных сетей этот совет прозвучит несколько странно. Но ведь вашим

клиентам, а тем более вашим работодателям не нужно знать ваш личный статус или домашний адрес, верно? Им нужно знать ваш профессиональный опыт, а также то, как с вами связаться. Вы ж, надеюсь, не раздаете ваш домашний адрес и телефон прохожим на улице? Значит не стоит ее раздавать незнакомым людям в сети.

Не отключайте настройки конфиденциальности

Будьте внимательнее! Периодически проверяйте настройки конфиденциальности. Многие социальные сети любят менять настройки без предупреждения. Маркетологи, как и взломщики, очень любят знать о вас как можно больше. Откуда получить эти данные? Проще всего посмотреть в социальной сети, которой вы пользуетесь. Безусловно, настройки конфиденциальности достаточно сложно найти на сайтах соцсетей. Это сделано специально. Еще сложнее простому пользователю понять, что можно изменить, а что нет. Потому большинство оставляет их по умолчанию. Это неправильно!

Не шляйтесь где попало!

Да-да, именно так! Вы ж не гуляете по неосвещенным опасным улицам ночью? Ну а почему вам так хочется посетить сайты с сомнительным содержимым? Ведь ловушек там не меньше! Будьте умнее! Не давайте злоумышленникам повод!

Используйте безопасное соединение VPN

Если вам приходится использовать интернет в общественном месте, помните, что вы не можете проконтролировать его безопасность! Ваше интернет-соединение – это ваше уязвимое место. Если вы не можете гарантировать его безопасность – лучше не используйте его! Ну а если все же очень нужно? Тогда используйте безопасное соединение VPN и тогда никто не сможет отследить ваш трафик (ну, разве что от конечной точки VPN до вашего сайта, который вы посещаете, но вероятность этого все же гораздо меньше).

Будьте внимательны при загрузке

Главная цель киберпреступников – заставить вас загрузить вредоносное ПО –программы или приложения, которые несут вредоносное ПО или пытаются украсть информацию. Это вредоносное ПО может быть замаскировано под приложение: от популярной игры до того, что проверяет трафик или погоду. Подумайте, прежде чем запускать приложение (игру) с непонятного сайта. Особенно советую думать пользователям Android, загружающим ПО с непонятных репозитариев.

Используйте надежные пароли

Откровенно? Уже надоело говорить о паролях. Понимаю, что вы не можете их запомнить, но ведь есть такое программное обеспечение как «менеджеры паролей», при этом вам необходимо запомнить всего лишь один – мастер-пароль. Фактически пароль к вашему хранилищу паролей. Какой использовать – выбирать вам. Но постарайтесь задуматься!

Второй выход из ситуации с паролями – использование MFA – мультифакторной аутентификации. Причем просьба заранее подумать, что второй фактор не должен использовать SMS. Это может быть генератор на вашем смартфоне или (что еще лучше) – аппаратный токен (ключ).

Совершайте покупки в Интернете с безопасных сайтов

Каждый раз, покупая что-либо в Интернет, вы предоставляете информацию о вашей банковской карте или вашем банковском счете. Задумайтесь о то, где и кому вы даете эту информацию. На мой взгляд, гораздо удобнее использовать «виртуальную» карту. То есть карту, которая существует только в Интернет. Причем на ней должен быть в лучшем случае неснижаемый остаток, а то и вообще не должно быть денег совсем. Т.е. алгоритм ваших действий достаточно прост: на сайте вашего банка вы переводите нужную сумму со своей реальной карты на виртуальную. Затем расплачиваетесь виртуальной картой и снова на сайте банка перекидываете остаток обратно на реальную. В результате – даже если злоумышленник что-то узнает о

виртуальной карте – на ней 0. А при любой опасности вы закрываете виртуальную карту и открываете ее снова. При этом к ней привязан другой (виртуальный) счет.

Будьте осторожны с тем, что публикуете

Любой комментарий или изображение, которое вы публикуете в сети, могут оставаться в сети навсегда, поскольку удаление оригинала (например, из Twitter) не приводит к удалению копий, сделанных другими людьми. У вас нет возможности «забрать назад» замечание, которое вы бы не сделали, или избавиться от смущающего селфи, сделанного на вечеринке. Не размещайте в Интернете ничего, что вы бы не хотели, чтобы увидела ваша мама или потенциальный работодатель.

Будьте осторожны с тем, кого вы встречаетесь в Интернете

Привыкайте, ваши интернет-знакомые могут в жизни быть совсем другими людьми! Более того, в настоящем мире подобных людей может никогда не существовать!

Своевременно обновляйте программное обеспечение

Как ни банально прозвучит, но используйте лицензионное программное обеспечение и своевременно его обновляйте! Безусловно, это не защитит вас от всех проблем, но резко снизит вероятность их возникновения.

Постарайтесь не забывать об этих правилах и обязательно учите этому ваших близких.