10 простых советов по безопасности в Интернете

1 Не доверяйте каждому письму, которое Вы получили

Некоторые кибер-преступники могут выдавать себя за другого человека, чтобы получить и украсть Вашу персональную информацию. Итак, как Вы можете узнать, что Вас обманывают? Самый простой способ – это перестать общаться с людьми, которых Вы не знаете. Также Вам не следует нажимать на ссылки, которые Вы получили от неизвестных людей. Кроме того, можно доверять только веб-сайтам, которые начинаются с https:// (у таких сайтов в адресной строке браузер, где написан адрес сайта, показывается замочек). Никогда не предоставляйте Вашу персональную информацию сайтам с другими обозначениями. Более того, Ваш банк никогда не будет спрашивать Ваш адрес электронной почты, так что не сообщайте эту информацию в таких случаях.

2 Будьте осторожны с загрузкой вложений

Если Вы по электронной почте получили от неизвестного человека письмо с вложениями (как правило, это файлы с расширениями .zip, .rar, .exe, документ Word, или, казалось бы, невинная фотография), никогда не открывайте их (не скачивайте). Такие вложения могут содержать вредоносные программы, которые могут инфицировать Ваш компьютер. К сожалению, даже приходится опасаться писем от друзей, потому что сами того не желая, они могли отправить Вам вредоносную программу. Лучше всего, перед тем как открывать такие вложения, уточнить у них, действительно ли они отправляли Вам письмо и что там вложено.

3 Безопасно посещайте сайты в Интернете

Не предоставляйте просто так Вашу персональную информацию любому веб-сайту, не задумываясь над тем, зачем он это спрашивает. Вам также следует доверять Вашему браузеру, т.к. если на сайте существует что-либо подозрительное, то он сообщит Вам о том, что данный сайт является потенциально опасным. Обязательно обратите на это Ваше внимание.

4 Используйте различные пароли и регулярно меняйте их

Если Вы хотите зарегистрировать себя на надежном и внушающем доверие сайте, обязательно используйте пароль, который сочетает в себе буквы, цифры и символы (хотя некоторые веб-сайты специально попросят Вас об этом). Никогда не используйте одинаковый пароль для всех Ваших аккаунтов. Регулярно меняйте Ваши пароли. Кроме того, не отправляйте Ваш пароль другим людям и не оставляйте его записанным где-либо. Это может показаться немного экстремальным, но Вам необходимо остановить других людей, которые попытаются получить доступ к Вашим устройствам, аккаунтам и сети.

5 Будьте осторожны с СМС

Кибер-хакеры теперь используют этот сервис отправки сообщений для выполнения своих атак, поэтому Вам также стоит быть предельно внимательными с тем, что содержат данные сообщения. Обращайте пристальное внимание на СМС от Ваших Банков, особенно если Вы не совершали операций.

6 Установите антивирус на все Ваши устройства

Предоставьте экспертам возможность заботиться о безопасности Вашего компьютера или смартфона, позволяя антивирусной программе присматривать за ними и защищать Ваши устройства от вредоносных программ. Антивирус поможет Вам обеспечить безопасность при совершении онлайн-покупок и позволит Вам не беспокоиться при просмотре веб-сайтов.

7 Проявляйте осторожность в общественных Wi-Fi зонах

Очень часто, когда Вы находитесь на вокзале, в кафе или в гостинице, Вы можете совершенно бесплатно подключиться к Wi-Fi. Хоть это и очень удобно, имейте в виду, что данная сеть является публичным соединением, а потому Вам следует быть предельно внимательным по отношению ко всему, что Вы делаете во время такого подключения. При просмотре сайтов обращайте внимание на то, присутствует ли значок замочка в адресной строке Вашего браузера рядом с адресом сайта. Также мы не советуем Вам осуществлять банковские транзакции при подключении к общественному Wi-Fi.

Удаляйте следы Вашего пребывания, если Вы работаете на чужом компьютере

Если Вы подключились к персональному почтовому аккаунту при использовании чужого компьютера, не забудьте удалить всю историю просмотра сайтов, включая куки. Удалите скаченные файлы из загрузок и корзины.

Разрешите обновления Ваших программ и операционной системы

Если Ваша операционная система или любое из приложений, установленные на Вашем компьютере, сообщают Вам о том, что доступны новые обновления, прочитайте внимательно данное сообщение и установите их. Даже если вам потребуется адаптироваться к каким-либо изменениям, все равно лучше иметь обновленную версию, т.к. она будет содержать последние обновления от разработчика в плане безопасности.

Оплата в сети Интернет

Любые покупки в сети Интернет проводите только с использованием протокола 3D Secure (подтверждение операций с использованием одноразового кода). Это позволит Вам обезопасить свои средства от кибер-преступников. Также не сохраняйте данные своей карты на малоизвестных сайтах.