**Десять золотых правил безопасности при работе в сети Интернет**

Безопасность в Интернете не имеет возрастных ограничений, и каждый из нас может защитить себя от кибер-преступников, не будучи экспертом в этих вопросах. УВД Миноблисполкома подготовило десять золотых правил, которым необходимо следовать, чтобы обезопасить себя в Интернете: Также подготовлены рекомендации по соблюдению мер информационной безопасности при обращении с банковскими платежными картами.

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.

1. **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.

1. **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.

1. **Используйте различные пароли и регулярно их меняйте**

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.

1. **Избавьтесь от назойливой рекламы**

Вы никогда не знаете, что может сделать Ваш невинный клик в то время, пока Ваш браузер наполняется назойливыми баннерами, всплывающими окнами и рекламными объявлениями, которые Вы не хотите видеть. Чтобы избавиться от них, установите соответствующий сервис, блокирующий рекламу, например, Adblock.

1. **Будьте осторожны с SMS-сообщениями**

Кибер-хакеры теперь используют этот сервис отправки сообщений для выполнения своих атак, поэтому Вам также стоит быть предельно внимательным с тем, что содержат данные сообщения. Несколько месяцев назад мы столкнулись с вредоносной программой, которая распространялась в виде SMSс одним простым вопросом типа «А это твоя фотка?». Как только жертва нажимала на ссылку, на устройство устанавливалось приложение, которое было способно шпионить за его контактами.

1. **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.

1. **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.

1. **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.

**10. 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.

УВД Миноблисполкома