**13 простых правил, которые помогут вам не стать жертвой киберпреступления**

Киберпреступность – понятие относительно новое: первое официальное упоминание о хакерах было обнародовано в 60-х годах прошлого века. Речь шла о группе пытливых студентов Массачусетского технологического института, которые манипулировали программами на новом университетском компьютере. Однако в те годы компьютерные преступления нельзя было назвать киберпреступлениями, хоть преступники и назывались хакерами. Но интернетом в то время и не пахло, а компьютеры не были объединены одной сетью. Да и цена, а также размеры одной ЭВМ были очень внушительными, так что все компьютерные преступления сводились исключительно к финансовым махинациям, связанным с ценой самого компьютера, а это несколько миллионов долларов.

Развитию киберпреступности поспособствовало стремительное распространение интернета в 90-х годах, когда и персональный компьютер, и интернет стали наиболее доступными для обычных граждан. С тех пор границы реального и виртуального миров с каждым днем становятся все более размытыми, а киберпреступники – все более изобретательными. Далеко не каждый человек осознает реальную угрозу, которой себя подвергает, выходя во Всемирную Паутину, ведь мы не просто ежедневно выходим в интернет, мы там практически живем: пересылаем друг другу важную информацию, выкладываем фотографии, пользуемся геолокацией, продаем и покупаем. Наши персональные и финансовые данные мы ежедневно предоставляем различным сайтам и, не задумываясь, жмем лайки, ссылки и картинки. Потому что интернет – это удобно. Но это удобно не только обычным пользователям, но и преступникам, ведь если подумать, то запустить программу-вымогателя Wana Cry ransomware, которая в 2017 заблокировала работу нескольких компаний в Великой Британии, мог обычный пользователь, необдуманно нажавший на кнопку в письме.

Но финансовые аферисты – это наименьшее из зол, с которым можно столкнуться. К примеру, благодаря системе «Умный дом» взрывающийся холодильник или микроволновка становятся вполне реальной угрозой, а если подумать о системе «Умный город», когда каждый предмет в городе подключен к Сети, контролирующей все окружающее, вообще становится страшновато. Но, несмотря на огромный потенциал для киберпреступников, «Интернет вещей» становится все более популярным, поскольку удобства такого пользования бытовой техникой действительно освобождают массу времени.

Интернет оказывает большое влияние на жизнь каждого человека, который им пользуется.Кибертерроризм – проблема всемирного масштаба, но кибербуллинг становится проблемой одного человека. И защитить себя в Сети очень сложно. Преступность с улиц уверенно перебирается в интернет: торговать оружием, наркотиками и людьми в Dark web значительно проще, чем в реальности, и управлять общественным мнением с помощью ботов менее затратно и менее хлопотно, нежели с помощью живых пиарщиков.

**Как защищает государство?**

Сталкиваясь с преступлением в реальной жизни, человек обращается в правоохранительные государственные органы, призванные бороться с преступностью и защищать граждан своей страны. Но что делает государство для обеспечения нашей безопасности в интернете?И кто занимается предотвращением киберпреступлений?

Защита персональных данных пользователей регулируется на государственном уровне с целью предотвращения шпионажа, шантажа, вымогательства, финансовых манипуляций и прочих преступлений. К примеру, в 2010 году правительства некоторых стран (Китай, Россия, Индонезия, Южная Африка и др.) обязали компании, работающие с персональными данными пользователей – медицинские, финансовые, кредитные – размещать свои сервера исключительно на территории страны проживания. С одной стороны, это должно исключить кибершпионаж, а с другой – все пользователи с их персональными данными всегда как на ладони у правительства и полиции. А в США и Чили полная свобода передачи данных, но доступ к ним третьих лиц возможен исключительно по решению суда, зато в США уже более 100 лет существует закон, разрешающий вводить санкции против других стран при необходимости. В Украине вводятся санкции точечно, как в случае с отключением Яндекса и Вконтакте. В Канаде вообще нет никаких ограничений для передачи информации.

**Как защитить себя**

Говоря о киберпреступности, необходимо понимать, что технический прогресс играет на руку преступникам.  Всего один человек с ноутбуком способен нанести колоссальный ущерб как большой компании, так и конкретному человеку и с большой долей вероятности остаться безнаказанным. Специалисты по кибербезопасности всегда должны работать на опережение, но хакеры время от времени выигрывают эту битву. Поэтому крайне важно, чтобы пользователи интернета сами повышали собственный уровень безопасности, тем самым повышая его в целом. Для этого, по словам специалистов, всегда необходимо придерживаться элементарных правил кибергигиены, о которых все знают, но часто игнорируют:

1. Использование антивирусных программ.
2. Использование сложных уникальных паролей для каждой службы.
3. Регулярное обновление программного обеспечения. Используя его уязвимости, преступники легко могут получить доступ к компьютеру.
4. Ограничение личной информации в соцсетях: фотографии, имена и фамилии, родственные связи, места отдыха, домашний адрес, ваш банк, номер телефона и т.д.
5. Регулярно проводите беседы с детьми о правилах поведения в интернете, особенно в соцсетях. Ваши дети должны знать о недопустимости любого негативного воздействия на них и необходимости сообщить родителям о подобных инцидентах.
6. Отслеживайте информацию о нарушении безопасности ваших данных на сайтах, на которых вы зарегистрированы, особенно если через эти сайты ведется коммерческая деятельность.
7. Никогда не открывайте письма на электронной почте, если не уверены в отправителе.
8. Не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут.
9. Не подключайтесь к сомнительному WiFi.
10. Не подключайте чужие USB-носители.
11. Не предоставляйте возможность физического доступа к вашим устройствам. Относитесь к вашим устройствам, как к кошельку с кучей денег, потому что так оно и есть на самом деле – информация стоит дорого.
12. Проверяйте информацию, прежде чем в нее поверить.
13. Проверяйте аккаунт пользователя, прежде чем добавлять его в друзья.

Если вы стали жертвой киберпреступников, вы должны сообщить об этом в полицию. Даже если вам кажется, что это незначительное мошенничество, вполне вероятно, что вы поможете обезвредить профессиональную группу хакеров. В конце концов, борьба с киберпреступностью – это дело каждого.