Что включает в себя кибергигиена

Кибергигиена - это набор ежедневных привычек, знаний и навыков, которые позволяют существенно снизить риски работы в Интернете Поговорим о том, из чего они складываются.

В первую очередь это знание угроз, с которыми можно столкнуться в Интернете. Предупрежден - значит вооружен.

За чем же охотятся злоумышленники? Это могут быть:

- Деньги в чистом виде. Переведи мне деньги, подпишись на платную рассылку, проголосуй (и мелким шрифтом *стоимость голосования 100500 рублей). Реализуется, как правило, путем ввода данных банковской карты или номера телефона. Сюда же ключи к банковским сервисам: SMS с кодом от банка, CVV-код с обратной стороны карты и пр. Отсюда вывод - вводить эти данные, только если абсолютно уверены в надежности сайта. Никому, никогда не сообщать пин-код, SMS-код и CVV-код.
- Важные для вас данные, чтобы потом вас шантажировать. В последние годы прокатилась волна так называемых "шифровальщиков" - вирусов, которые зашифровывают все данные на жестком диске и требуют плату за ключ для расшифрования. Сейчас эта тенденция идет на спад, т.к. люди предпочитают мириться с потерей данных, чем платить злоумышленникам; кстати, получив деньги они не всегда могут расшифроваться файлы обратно. Сюда же - блокировка телефона через Apple ID на iPhone или учетную запись Google на Android, шантаж личными фотографиями другим компроматом и пр.
- Ваш компьютер. Если злоумышленник получит контроль над компьютером, он сможет использовать его в своих целях тайно от нас! Рассылать с него вирусы, майнить криптовалюту, взламывать сайты, а если наберет таких компьютеров несколько сотен - сможет завалить любой сайт, направив на него потоки мусорных запросов. Угадайте, к кому придут правоохранительные органы... Доказывайте потом что вас тоже взломали.
- Персональные данные: паспорт, СНИЛС, ИНН, другие документы. Имея эти данные, мошенники имея сообщников в банке или МФО могут оформить на вас кредит, или прикрепить вас к левому пенсионному фонду.
- Ваша личность. Так пишут в современной англоязычной литературе - Identity. Это ваша страничка ВКонтакте, FaceBook или Одноклассниках, электронная почта, месенджеры. В этом случае от вашего имени можно, например, размещать рекламу, в том числе чего-нибудь запрещенного: наркотиков или средств для увеличения какого-нибудь органа. Или использовать для классической рассылки "Друг, я в беде, пришли деньги". Накрутить рейтинг, сделать видимость посещаемости страницы, оставлять от вашего имени комментарии... В общем, вести себя так, как вы бы себя никогда

не повели, попутно испортить вашу репутацию и подставить знакомых.Защититься можно соблюдая несколько правил, поговорим об этом в дальнейших выпусках.

- Почта, телефон, логин, другие контакты. Чтобы рассылать рекламную рассылку (спам). А еще логины и адреса почты продают большими пачками хакерам, которые пытаются их взломать. Какой-то процент успешных взломов у них есть.
- Информация о человеке и его жизни. Например, из социальных сетей можно понять, где человек живет, какой его уровень достатка, какие вещи есть в его квартире и когда он уехал в отпуск. Как раз достаточный набор данных, чтобы запланировать квартирную кражу. Что характерно, человек сам выкладывает эти данные о себе.
- Недавно был скандал с раскрытием местонахождения секретной американской базы. Солдаты во время пробежки включали трекеры (программа, которая по GPS определяет маршрут бега, расстояние, скорость, подъем - удобная штука для спортсменов). Но эта же программа ведет статистику по местам скопления бегунов. Так вот, горячая точка, пустыня, вокруг ничего... и жирный круг на карте от множества частых пробежек солдат вокруг базы.

Зачем мошенникам нужен простой пользователь?

Можно захватить и использовать компьютер простого пользователя, вынудить его заплатить деньги или украсть аккаунт в соцсетях.

Современные методы мошенничества массовые, ориентированы на широкий круг пользователей. Так сказать, бьют по площадям. Работают в основном наудачу: если из ста пользователей хотя бы несколько повелось - уже хорошо.

Например:

- Мошеннические сайты.
- Сообщения рассылки с просьбой прислать деньги, зачастую от взломанных аккаунтов ваших знакомых.
- Компьютерные вирусы - атакуют всех без разбора. Но при этом достаточно тупы, знают один или несколько способов атаки и достаточно быстро попадают в базу антивирусов.
- Программы для подбора (угадывания) паролей.

Таким образом, в Интернете постоянно работают вредоносные программы, атакующие всех без разбора, и злоумышленники, атакующие всех подряд по типовому шаблону. И вот в их область действия попадают все без исключения.

Так что хотите вы или нет, защищаться вам придется.

И тут как в анекдоте есть две новости: хорошая и плохая. Плохая заключается в том, что целью мошеннических действий или атак может стать любой. А хорошая - в том, что защититься от угроз не так сложно, как многим кажется.

Безопасность своей учетной записи.

Под учетной записью в материалах по информационной безопасности понимается ваша страничка в социальных сетях, почта, имя пользователя компьютера - в общем любое имя пользователя (логин), для которого вы вводите пароль. В дальнейшем мы будем использовать этот термин.

Важно, чтобы никто не знал ваш пароль, а также не мог его подобрать; при этом желательно чтобы вы сами его не забыли и не потеряли.

Помните, что логин и пароль - это как главные ворота замка, именно на них будет направлен первый штурм. И если общие механизмы защиты (стены и башни замка) предоставляются системой или сайтом: блокировка после нескольких неуспешных попыток, ограничение времени между двумя попытками, проверка "Я не робот" - то сложность пароля и корректное с ним обращение (как выучка и реакция защитников замка) - зависят полностью от нас.

Если защитников нет, никакие стены не помогут.

Защита от компьютерных вирусов, шифровальщиков и других вредоносных программ. Важно знать, как определить наличие вируса, как правильно работать с антивирусными программами, что делать в случае подозрения на заражение.

Защита от вредоносных почтовых рассылок и фишинговых сайтов.

Фишинговые рассылки содержат файлы, которые выглядят как обычные документы, но на самом деле являются программами. Едва вы попытаетесь их открыть, эти программы запустятся от вашего имени и начнут выполнять свои функции, как правило, предоставлять доступ к вашему компьютеру или телефону. А поскольку вы запустили их от своего имени, злоумышленник будет иметь те же права доступа, что и вы. Или как вариант такие письма могут содержать ссылки на фишинговые сайты.

Фишинговые сайты - это сайты, которые выглядят точь-в-точь как настоящие, и рассчитаны на то, чтобы вы ввели в них свои логин и пароль - тогда они попадут к злоумышленникам. Их бывает очень сложно отличить от настоящих, но всегда есть какая-нибудь зацепка.

Фишинг - это от слова fishing, рыбалка. Наживка - это отправленный по почте файл или фальшивый сайт. А рыбка - это простые пользователи.

Навыки безопасной работы в Интернете, подключения через беспроводные сети, умение защитить ваш компьютер и телефон от взлома, сделать их невидимыми и практически не взламываемыми (практически - потому что в теории их конечно можно будет взломать, но те, кто это сможет сделать, нами не заинтересуется, а те, кто заинтересуется - не смогут)

Умение распознавать действия мошенников и не играть им на руку. В первую очередь твердо знать, куда вводить свои данные (в том числе логин и пароль), а куда нет. Уметь отличать мошеннические сайты от настоящих. Распознавать файлы "с сюрпризом" и не запускать "троянских коней". Не вестись на слезные просьбы "друзей" и "родственников" и не переводить им деньги, не убедившись предварительно что они те, за кого себя выдают.

Управление данными. Контроль их распространения, контроль доступа к ним, а также резервное копирование.

Большая часть утечек личных и рабочих данных случается в результате небрежности самих их владельцев.

Например, недавний громкий скандал об утечке персональных данных в МФЦ "Мои документы" связан с тем, что хозяева документов, воспользовавшись общими компьютерами чтобы загрузить свои документы в систему, забывали удалить с них свои документы. В результате на общих компьютерах в МФЦ хранился большой архив "забытых" документов, которые любой посетитель мог скопировать себе на флешку.

Навыки работы с теми программами, системами и сайтами, с которыми вы работаете (раз уж вы окрасили себя в те цвета, в которые окрасили). Важно четко понимать, что вы делаете, и вовремя распознать ситуацию, когда что-то пошло не так. Не поленитесь потратить время и изучить свой компьютер, рабочие программы, научиться слепому десятипальцевому методу набора на клавиатуре, развить моторику работы мышью.

Источник:
https://zen.yandex.ru/media/id/5c595835c2e36000adb6fb7e/chto-vkliuchaet-v-sebia-kibergigiena-5c73dc43a66f1a00b4e591c3