Кибергигиена. Что каждый должен знать о своих персональных данных

Хакеры сливают в сеть гигабайты частных переписок, фотографий и файлов, которые многие просто не умеют защищать.

Персональные данные — золото XXI века. Это нужно осознать лучше раньше, чем позже.

«Мне нечего скрывать» — фраза, с которой начинаются большие проблемы. Именно в ней заложены огромные риски для вашей карьеры, бизнеса, личной жизни и даже будущего ваших детей.

Когда Интернет знает вас лучше, чем вы сами, вы попадаетесь не только на маркетинговые уловки, но и на удочки к мошенникам.

Люди по всему миру поняли, насколько важно правильно мыть руки, только, когда случилась пандемия коронавируса. Цифровой гигиене можно и нужно научиться вовремя.

Кибергигиена — это соблюдения простых правил цифровой безопасности при работе с интернетом. Она не менее важна, чем личная гигиена для каждого человека. Ее важно соблюдать на уровне ежедневной привычки, чтобы защитить себя и своих близких от хакеров в интернете.

Хакеры — интересные персонажи. О них снимают фильмы, ходят легенды, их мало кто видел, но слышали об их деятельности практически все. На самом деле, хакеры — это высококвалифицированные IT-специалисты, которые обладают особым мышлением. Если обычный программист думает, как создать хорошо работающий продукт, то хакер смотрит на задачу нестандартно.

Для примера и сравнения, проведем аналогию с обычным стаканом. Программист использует стакан, чтобы налить в него воду и выпить. Хакер же будет изучать его, переворачивать, стучать по нему, бросать на пол и пытаться найти трещины. Хакер — это охотник, фанат (в хорошем смысле) своего дела, который днями напролет может сидеть над задачей, пытаясь разгадать загадку, обойти систему защиты или антивирус.

Существуют два типа хакеров

Black hat — плохой, «черный» хакер, который взламывает программы и другие системы с целью наживы и кражи информации.

White hat — «белые» хакеры, второй тип, который противостоит в цифровом мире «черным» взломщикам. По сути, они обладают одинаковым набором знаний, но «белые» хакеры — это этичные эксперты, которых

нанимают организации, чтобы взломать и проверить собственную систему, а затем закрыть существующие уязвимости. Этот способ защиты является самым эффективным и практичным для проверки своих ресурсов от Black hat хакеров.

«Думать, что вас не взломают, потому что у вас нет ничего интересного — категорически неверно и очень опасно»

У каждого человека есть его личные данные, которыми он ежедневно делится в интернете. Эти данные — личная собственность. За ними стоят конкретные истории людей, их покупок, предпочтений, финансов или даже болезней. То есть речь идет о чувствительной информации. Если придать ее огласке — можно испортить кому-то репутацию или изменить судьбу человека. Когда мы доверяем эти данные третьим лицам или государственным органам, — нужно быть уверенным, что вашу собственность будут хранить в безопасном месте, соблюдая все стандарты безопасности.

Представим, что заинтересованному лицу нужно дискредитировать суд присяжных, которые слушают какое-то важное дело. Вариантом может быть следующий сценарий. Злоумышленник получает номера банковских карт участников процесса (вспомните, сколько раз вы пересылали номер своей карты). Затем можно разослать каждому на карту определенную сумму денег и написать что-то вроде «Спасибо, как договаривались — ваш аванс за решение».

Остается лишь сделать эту историю получения «вознаграждения» публичной. Так суд присяжных окажется в неудобной ситуации, а возможно, и будет заменен вовсе.

Этот пример демонстрирует, как любая информация о каждом из нас может быть использована против нас же довольно простым способом.

Наблюдаются также массовые сливы информации, они могут быть вследствие нескольких причин. Вас могут взломать лично, или атаке подвергнется сайт госоргана, которому вы доверили данные. Так, если вы доверяете свои деньги банку, — предполагаете, что банк отвечает за их сохранность. Это значит, что перед тем как доверить личные данные третьим лицам, стоит спросить у них, кто их защищает. А также и кто ответит, если эти данные окажутся в открытом доступе.

Чтобы защититься от взлома, достаточно придерживаться стандартных правил кибергигиены:

- Использовать разные пароли для разных аккаунтов, при этом необязательно помнить их все — можно просто хранить их в специальных пассворд-менеджерах;

- Создавать сложные пароли;
- Использовать двухфакторную аутентификацию через приложение, а не смс;
- Не открывать незнакомые ссылки в переписках по почте и смс;

Думать, что вас не взломают, потому что у вас нет ничего интересного — категорически неверно и очень опасно.

Злоумышленник может взламывать вас, чтобы атаковать с вашего аккаунта вашего коллегу по работе или родственника. Поэтому позаботьтесь о себе и ваших близких — защитите свои аккаунты.

«Эффективней и дешевле позаботиться о своей безопасности до того, как вас попробуют взломать»

Однажды, один известный успешный предприниматель, в компании наших общих друзей и партнеров предложил мне пари. Он заявил, что я не смогу снять с его карты деньги в течение получаса, поскольку у него стоит подтверждение транзакций через смс, и Mastercard надежно защищена. Тогда моим ребятам понадобилось около 10 минут, чтобы снять оговоренную с ним сумму. Это были небольшие деньги $200-300, и это было просто.

Злоумышленники же обычно выбирают свою жертву и готовятся к хищению средств. Для этого им необязательно взламывать банк. Обычно им достаточно иметь о вас немного информации, сделать клон вашего номера телефона и подтвердить крупную транзакцию через смс. После этого, деньги быстро отмываются через криптовалюты или специальные обменники. В таком случае найти виновного очень сложно.

Намного эффективней и дешевле позаботиться о своей безопасности до того, как вас попробуют взломать. Мышление злоумышленника работает таким образом, что при виде решеток на окнах он не будет пытаться туда залезть. Ведь вокруг полно окон без решеток. То же самое и в кибербезопасности. Если у вас соблюдены элементарные правила кибергигиены — будьте спокойны, вероятность взлома ваших аккаунтов падает в десятки раз.

Около 90% инцидентов в финансовом секторе распределяются в трех основных направлениях:

- атаки веб-приложений,
- атаки распределенного отказа в обслуживании (DDoS),
- клонирование платежных карт.

Цель таких атак обычно:

- украсть данные,
- украсть деньги,
- мониторинг активностей клиента,
- срыв сделки.

«Обучение детей поведению в интернете — неотъемлемая часть воспитания ребенка»

Конечно, все мы хотим, чтобы наши дети развивались вместе с технологиями. У них куча девайсов и постоянная возможность общаться с друзьями онлайн: соцсети, TikTok, Instagram, Snapchat и много других приложений. Без них, надо признать, их жизнь будет не такой насыщенной и интересной.

Пока родители приспосабливаются к новым реальностям, дети самостоятельно путешествуют по интернету и оказываются уязвимыми для незнакомцев. Известны тысячи случаев, когда взрослые злоумышленники создают фейковые аккаунты, выдавая себя за подростков и входят в контакт с детьми, общаясь с ними напрямую.

Для того, чтобы защитить своих детей от подобных ситуаций, существует несколько действенных способов, взаимно дополняющих друг друга.

Обучение детей поведению в интернете — неотъемлемая часть современного воспитания ребенка. К ним относится родительский контроль техническими решениями, которыми можно ограничивать и контролировать действия ребенка в интернете. Такими инструментами являются Umobix, Bark и другие приложения, которые позволяют защитить вашего ребенка от неожиданных и ненужных знакомств.

В интернете неподготовленный ребенок может допустить к себе человека с не самыми лучшими намерениями.

5 основных опасностей, с которыми дети сталкиваются в Интернете:

1. Общение злоумышленника с вашим ребенком в приватных сообщениях с фейковых аккаунтов.

2. Кибербуллинг, троллинг, моббинг (травля в интернете).

3. Онлайн-хищники — люди, которые совершают сексуальные надругательства над детьми. Обычно они либо начинаются, либо полностью происходят в Интернете.

4. Размещение личной информации. Дети еще не понимают социальных границ, размещают в Интернете информацию, позволяющую установить личность, домашних адресов или планов семейного отдыха.

5. Случайно загружается вредоносное программное обеспечение.

«В связи с переходом на удаленную работу, во всем мире наблюдается рост хакерских атак и утечек информации»

Мир уже не будет прежним. Пандемия и ее последствия кардинально изменили все вокруг. Люди начали работать удаленно, используя каждый день групповые чаты, платформы обмена данными и видеоконференции. Мы уже не представляем свою жизнь без интернета. Многие осознали, что такая работа значительно практичней: можно сэкономить кучу времени, не передвигаясь со встречи на встречу в пробках. Это позволило нам выйти на новый уровень эффективности.

Более того, многие отмечают, что работа и коммуникация с коллегами онлайн стали значительно результативнее и быстрее, чем раньше.

К сожалению, вместе с новыми технологиями приходят и новые угрозы. Во всем мире наблюдается рост хакерских атак и утечек информации. Это означает, что каждый ответственный бизнес должен уделить внимание безопасности до того, как им заинтересуются злоумышленники. Ответственный подход к вопросу кибербезопасности — это конкурентное преимущество на рынке и забота о своих клиентах.

Самые распространенные киберугрозы для бизнеса:

1. Фишинговые атаки

Самая большая, самая разрушительная и самая распространенная угроза для бизнеса — это фишинговые атаки (90% всех атак).

Фи́шинг — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям

2. Вредоносные атаки

Вредоносное ПО — вторая большая угроза, с которой сталкивается бизнес. Он включает в себя различные киберугрозы, такие, как трояны и вирусы.

3. Интернет-вымогатели

Существует такой тип атак, как Ransomware. Он включает в себя шифрование данных компании, чтобы их нельзя было использовать или

получить к ним доступ, а затем вынуждает предприятие заплатить выкуп за разблокировку данных.

4. **Слабые пароли**

Еще одна большая угроза, с которой сталкивается бизнес, — это сотрудники, использующие слабые или легко угадываемые пароли.

5. **Инсайдерские угрозы**

Инсайдерская угроза — это риск для организации, вызванный действиями сотрудников, бывших сотрудников, бизнес-подрядчиков или партнеров.

Тема кибербезопасности сегодня касается каждого: предпринимателя, родителя, детей и чиновников. В связи с повышенным интересом к этому направлению, при поддержке Национальной Ассоциации Кибербезопасности, мы запускаем серию публикаций, в которых участники ассоциации будут раскрывать важные темы о киберугрозах, рассказывать об азах цифровой гигиены и учить противостоять мошенникам.

Источник: https://5sfer.com/kibergigiena-chto-kazhdyj-dolzhen-znat-o-svoih-personalnyh-dannyh-instrukcziya-belogo-hakera/