INIMÕIGUSTE
KESKUS

Конфиденциальность и защита данных

Каждый клик и твои данные имеют значение!

Перемещаясь по сети, совершая покупки или общаясь, ты постоянно оставляешь **цифровые следы**, что может иметь реальные последствия для твоей конфиденциальности и других прав. Тем не менее часто остается неясным, сколько наших данных фактически используется и распространяется.

Будь внимателен к данным! В цифровой среде все важнее становится знать, кто, почему и как обрабатывает твои данные, и ты имеешь право получить уведомление об их обработке. Это также относится к ситуации, когда различные учреждения или люди используют твои данные, чтобы оказывать на тебя влияние посредством рекламы или медиа-контента в социальных сетях. Например, ты когда-нибудь замечал, что когда ты ищешь развлекательные мероприятия или новый предмет мебели, во время серфинга в сети тебе начинает попадаться именно такая реклама? Многие компании собирают информацию о тебе и делятся ей, поэтому они умеют прогнозировать твое поведение и направляют тебе целевой и персонализированный контент, адаптированный именно к твоему поведению и интересам. Это называется **микротаргетингом** (англ. microtargeting). Видеть интересующий тебя контент отчасти может показаться удобным и заманчивым, но с другой стороны, ты можешь потерять свою бесценную конфиденциальность и даже больше. Платформы социальных сетей создали т. н. психологические профили для **персонализации** (англ. profiling) отображаемого контента, **оценивая** открытость людей к новому опыту, настойчивость, экстравертность, готовность к сотрудничеству и эмоциональную устойчивость. Обладая такими подробными данными, можно успешно влиять на пользователей, чтобы они покупали нужные вещи, кликали по определенным ссылками или совершали нужный выбор.

Помимо того, что ты можешь, сам того не зная, обнаружить, что развлекаешься в неизвестных сетевых ресурсах или покупаешь незапланированные вещи, экономика данных также может представлять угрозу для **демократии**. Знаешь ли ты, что те же методы использовались организаторами политических кампаний, чтобы адаптировать предвыборное сообщение к избирателю и таким образом повлиять на его голос?

Эта модель использовалась Cambridge Analytica, например, в предвыборной кампании Трампа и в преддверии голосования по брекситу. В таких процессах покупается ориентированная реклама, размещенная в Facebook с учетом предпочтений и ожиданий конкретных групп пользователей.

Более того, просмотр только тех новостей, которые совпадают с собственными взглядами лица, может привести к расслоению общества. Так оказывают влияние на людей, чтобы те вели себя определенным образом, а в результате это может привести к принятию общенациональных решений.

Для сбора данных используются, помимо прочего, файлы cookie.

Файлы cookie (или веб-трекеры)

Микротаргетинг работает с использованием электронных средств, таких как файлы cookie, плагины или отслеживающие пиксели (англ. tracking pixels). С помощью этих средств отслеживается твой веб-трафик – твои привычки, предпочтения и социальные связи в Интернете, – и создается твой профиль.

Файлы cookie – это данные, используемые веб-сайтами для хранения информации об их посещении. Файлы cookie бывают разных видов, как необходимые, так и нарушающие конфиденциальность: одни предназначены для управления посещениями веб-сайтов, другие – для персонализации веб-сайтов или для отслеживания и идентификации пользователей. Таким образом, файлы cookie используются, чтобы больше узнать о тебе.

Файлами cookie можно управлять в настройках конфиденциальности веб-браузера. Также можно пользоваться расширения браузера, которые помогают ограничить мониторинг веб-трафика. Чтобы ограничить микротаргетинг, просмотри настройки своих аккаунтов и социальных сетей.

В режиме инкогнито или режиме конфиденциальности история браузера, файлы cookie и временные файлы не сохраняются, но следует отметить, что в режиме инкогнито третьи лица могут перехватывать веб-трафик и отслеживать пользователей.

Для получения консультации по защите данных обратись к нам со своим вопросом или проблемой:

info@humanrights.ee

Утечки данных и кибероперации

В дополнение к сбору данных, например, с помощью файлов cookie все чаще организуют кибератаки на пользователей Интернета, чтобы таким образом получить наши данные, заразить компьютеры вредоносным программным обеспечением или, например, получить доступ к системам компании по неосторожности сотрудников. Для защиты данных важно, чтобы каждый применял на практике современные принципы кибергигиены и безопасности данных. Подробнее читай в главе о кибергигиене.

Ты имеешь право знать, кто оказывает на тебя влияние и как используются твои данные.

1. Конфиденциальность и защита данных

Что такое конфиденциальность?

Право на конфиденциальность защищает личную и семейную жизнь, неприкосновенность дома и тайну сообщений. Конфиденциальность также является частью общего права человека на свободное самоопределение, то есть права самостоятельно решать и определять, кто ты и какой образ, который ты создаешь. Каждый имеет право решать, делиться ли своей частной жизнью с другими людьми, компаниями, общественностью или государством, и в какой степени. Информационное самоопределение особенно подвержено риску в растущем обществе данных, где системы онлайн-платформ постоянно персонализируют наши сетевые среды и

предсказывают наше поведение, предпочтения и уязвимости. В то же время право на конфиденциальность действует online, а также offline.

Конфиденциальность не является привилегией для избранных или благом, которого ищут только известные люди. Это право, которое принадлежит **каждому**. Каждый человек имеет право на свободное самоопределение и на то, чтобы его личный выбор уважали другие люди, компании и государство.

Конфиденциальность поддерживает защиту других прав человека.

Право на конфиденциальность **защищает** физическую и психическую неприкосновенность человека и гарантирует его моральную и интеллектуальную свободу, репутацию и честь. Право на конфиденциальность защищает имя и идентичность человека от несанкционированного использования и раскрытия информации. Например, человек имеет право принимать решения, можно ли делиться публично своими изображениями и видео, и какими. Кража личных данных, например, в виде мошеннических аккаунтов, также запрещена.

Помимо этого, право на конфиденциальность защищает от произвольного шпионажа, слежки или преследования. Право на конфиденциальность также распространяются на **трудовую жизнь** лица – например, нельзя устанавливать камеры в раздевалке сотрудников, произвольно обыскивать кабинет юриста или разглашать информацию о здоровье сотрудника без разумного обоснования. Право на конфиденциальность защищает семейную жизнь лица и, таким образом, связаны с правом на вступление в брак и создание семьи (статья 12 Всеобщей декларации прав человека). В то время как статья 12 защищает право на вступление в брак, статья 8 защищает право на развод. Право на конфиденциальность распространяется и на защиту **семейной жизни**, защищая право на общение с ребенком. Право на конфиденциальность также защищает право выбирать социальные связи или добровольные сексуальные контакты и сексуальную идентичность. Нарушением конфиденциальности является, например, криминализация гомосексуализма, запрет на смену имени или пола или необоснованное ограничение выбора имени для ребенка.

Право на конфиденциальность также распространяется на **секретность сообщений**. Вмешательство в секретность сообщений допускается только в ограниченных случаях и при наличии конкретного оправдания. Запрещаются частная и произвольная разведка, обыски без четких границ и законных оснований, тайное прослушивание телефонных разговоров, вмешательство в голосовые/данные или запись разговоров. Обыск, проводимый полицией, также должен быть четко разграничен, основан на уважении человеческого достоинства и разрешен только в той мере, в какой это необходимо для достижения конкретной цели. Запрещается слежка за населением или скрытое хранение коммуникационных данных (в том числе в целях расследования тяжких преступлений). В своем законодательстве государство должно очень четко определить, в каких случаях вообще можно

использовать оперативно-розыскную деятельность и как в дальнейшем следует поступать с собранными данными.

Помимо обязанности государства воздерживаться от произвольного вмешательства в приватность лица, государство обязано обеспечивать эффективную защиту частной и семейной жизни граждан и предпринимать меры для ее защиты также в сфере взаимоотношений между людьми или средств массовой информации. Государство также должно защищать граждан от компаний, когда последние используют технологии или бизнес-модели, нарушающие права людей.

В каких случаях можно вмешиваться в частную жизнь человека?

Статья 8 Европейской конвенции о правах человека гласит:

„Каждый имеет право на уважение его личной и семейной жизни, а также тайны его дома и сообщений“

Никто не может произвольно вмешиваться в частную жизнь человека или осквернять его честь и доброе имя. В частную жизнь человека можно вмешиваться только в том случае, если это соответствует закону и если это необходимо в демократическом обществе в интересах национальной безопасности, общественной безопасности или экономического благополучия государства, для предотвращения беспорядков или преступлений, для защиты здоровья или нравственности, прав и свобод ближних.

Обоснование вмешательства в частную жизнь может исходить, например, из Уголовно-процессуального кодекса. Если человек совершил преступление, то при наличии разрешения следственный орган имеет право обыскивать дом человека с целью производства по делу о преступлении или подавать запросы обработчикам данных, например, банкам. Как запрос, так и обыск должны быть четко определены, и полиции нельзя произвольно интересоваться частной жизнью. Государство не должно вести массовое наблюдение за гражданами даже в целях борьбы с тяжкой преступностью и терроризмом, поскольку это непропорционально нарушит право людей на приватность.

Частная жизнь лица защищена следующими правовыми актами:

- на внутригосударственном уровне нашей Конституцией (ст. 26) и внутригосударственными судами;

- на международном уровне Всеобщей декларацией прав человека ООН (статья 12) и Международным судом;
- Европейской конвенцией о правах человека (статья 8) и Европейским судом по правам человека;
- Хартией основных прав ЕС (статья 7) и судом ЕС.

Что такое защита данных?

Каждый имеет право на защиту своих персональных данных. Право на защиту данных тесно связано с правом на конфиденциальность и стало особенно заметным с развитием технологий. С точки зрения защиты данных важными являются те части конфиденциальности, с помощью которых можно **идентифицировать** лицо и через которые лицо определяет себя по отношению к другим лицам и/или государству. Таким образом, личность человека является ключевой частью конфиденциальности. Идентичность – это то, что отличает человека от всех других людей, например, имя, идентификационный номер, присвоенный страной (например, личный код), этническая принадлежность, внешний вид, характер, поведение лица, его личное пространство, социальная сеть и т. д. Персональными данными считаются также личный адрес электронной почты, данные кредитной карты, данные связи или местоположения, получение социальной помощи или сетевые идентификаторы (например, IP-адрес или идентификаторы файлов cookie). Таким образом, твоими защищаемыми **персональными данными** являются все те данные, которые могут быть использованы для твоей идентификации.

Персональные данные особого типа – это те личные данные, которые нуждаются в особой защите, потому что в случае их утечки существует еще большая опасность для конфиденциальности лица. Персональными данными особого типа являются персональные данные, на основе которых выявляются расовое или этническое происхождение, политические взгляды, религиозные или философские убеждения или членство в профсоюзе, биометрические данные, используемые для уникальной идентификации физического лица (ДНК, геометрия лица, голос, отпечатки пальцев, отпечатки ладоней и глазные трансплантаты), данные о здоровье или данные о сексуальной жизни и сексуальной ориентации физического лица.

Технологии распознавания лиц (в т. ч. камеры слежения), которые обрабатывают персональные данные особого рода, широко используются, например, в Лондоне и Китае. Помимо поддержания общественного порядка, такие технологии могут использоваться для дискриминации или ограничения прав граждан. Также такие технологии затрагивают право жителей на конфиденциальность.

Каждый имеет право на защиту своих личных данных

Утечка личных данных, помимо потери конфиденциальности, может приводить к опасности для жизни, здоровья, краже личных данных, дискриминации, финансовому или репутационному ущербу. Таким образом, конфиденциальность защищает твою свободу пользоваться другими правами человека.

Статья 8 Хартии основных прав ЕС гласит: «**Каждый имеет право на защиту своих личных данных. Такие данные должны обрабатываться надлежащим образом, в определенных целях и с согласия заинтересованного лица или на иных правовых основаниях, предусмотренных законом. Каждый имеет право ознакомиться с собранными о нем данными и потребовать их исправления. Выполнение этих положений контролируется независимым органом**».

Более точные права и обязанности, связанные с защитой данных, предусмотрены в специальных правилах, например, в особой регуляции по защите персональных данных (англ. GDPR) и во внутригосударственном законе о защите персональных данных.

GDPR устанавливает общие принципы обработки данных: обработка должна быть законной, справедливой, прозрачной и целенаправленной; необходимо собирать, использовать и хранить как можно меньше данных, и данные должны храниться ровно столько времени, сколько необходимо; должна быть обеспечена правильность, точность и безопасность данных (доступность, целостность и конфиденциальность), а также ответственность.

Любая обработка данных должна иметь правовую основу. Одной из таких основ является твое **согласие**. Согласие на обработку твоих персональных данных должно быть дано добровольно, конкретно, сознательно и однозначно. Что касается согласия с различными услугами и средствами (например, файлы cookie) в социальных сетях, следует признать, что зачастую такая форма согласия не соответствует требованиям к его предоставлению – например, при нажатии на кнопку согласия пользователь часто не понимает, как его данные используются и кому передаются.

2. Права: твои данные, твой выбор

Твои данные важны. Твои данные являются валютой и ценностью сами по себе. Почти в каждом твоем взаимодействии с учреждениями проводится обработка данных, в ходе которой передаются твои личные данные, такие как имя, адрес,

дата рождения. Данные также передаются в онлайн-среде каждый раз, когда ты посещаешь веб-сайт, используешь поисковую систему, совершаешь продажу или покупку, пользуешься социальными сетями, отправляешь электронное письмо или просто скроллишь, свайпаешь, ставишь лайки или что-то постишь.

Обмен данными делает жизнь проще, удобнее и слаженнее. Но твои данные принадлежат тебе. Поэтому важно, чтобы они использовались именно так, как ты разумно представляешь себе обработку данных, а также хранились и обрабатывались безопасно.

Права

Право быть **информированным** об обработке своих персональных данных

- Учреждение должно уведомить тебя, если оно использует твои личные данные. Ты также имеешь право знать, кто, как и из каких источников получает данные, какие персональные данные обрабатываются, в каких целях и на
- каких правовых основаниях. Для этого учреждению необходимо предоставить условия защиты данных, и ты также имеешь право отправить их любому обработчику данных **запросы** о твоих данных.

- Кроме того, ты можешь использовать несколько баз данных (например, государственный портал eesti.ee или digilugu.ee), чтобы непосредственно увидеть, кто просматривал твои данные.

Право **отказаться** от обработки данных

- Часто ты имеешь право отказаться от обработки данных и использования твоих данных. Учреждение или другие лица, как правило, должны иметь твое согласие или какое-либо другое основание для обработки твоих данных. Государственная обработка данных в основном осуществляется на основании закона, и в этом случае согласие человека не требуется. Также в частном секторе, например, видеонаблюдение может быть оправдано законными интересами учреждения. Если для обработки данных требуется твое согласие, ты можешь отказаться от нее в любое время.

- Это также относится к публичному обмену твоими фотографиями или видео. Например, когда ты сам публикуешь чье-то фото или видео, всегда будет уместно спросить разрешения на это. Следует отметить, что разрешение также может быть отозвано в любой момент, и ты как автор обязан удалить фото или видео из публичных социальных сетей.

- Основанием для обработки данных являются: согласие лица, договор, юридическое обязательство, публичная задача, защита жизненно важных интересов лица или законный интерес.

- **Спам**. Также для осуществления прямого электронного маркетинга (т. е. спама) должно быть предварительное согласие клиента, которое можно отозвать (например, ссылка на отказ в конце электронного письма). Поэтому, если ты получил электронное письмо для продажи чего-либо, ты можешь попросить компанию прекратить это делать или обратиться в инспекцию по защите данных.

Право на **доступ** к своим данным и получение их копии

- Ты имеешь право знать, когда организация использует или хранит твои персональные данные, и получать копию собранных данных.
- Вы имеешь право требовать доступа к своим данным, собранным компанией или государственным органом. Ты также имеешь право выразить свои сомнения по поводу неправомерного использования твоих персональных данных.

Право на **исправление** своих данных

- У тебя есть право указать на любые ошибочные или измененные данные о себе, которыми обладает какая-либо организация.

Право быть **забытым**

- Ты имеешь право попросить организацию удалить данные, которые она хранит или использует о тебе безосновательно. Для изменения или удаления персональных данных обратись к первоисточнику. Если ты хочешь, чтобы поисковая система не отображала твои данные, ты можешь, например, запросить удаление личных данных через предоставленную форму.
- Твоя личность принадлежит тебе, и ты имеешь право принимать решения о своем образе как в физическом, так и в цифровом мире.

Право на **передачу** данных

- Ты имеешь право запрашивать в доступном и удобочитаемом формате данные, собранные учреждением о себе. Используя это право, ты можешь попросить одну компанию передать твои персональные данные другой компании, услугами которой ты хочешь пользоваться, например, в дальнейшем, но это должно быть технически возможно и осуществимо, если системы другой компании совместимы с системами первой.

Права в связи с **автоматизированным решением**

- Если в отношении тебя было принято автоматизированное решение с неблагоприятным воздействием или юридическими последствиями (например, искусственным интеллектом), т. е. решение о тебе было принято не человеком,

а, например, в результате анализа профиля с помощью инфотехнологических средств, тогда ты имеешь право запросить вмешательство человека в принятие решения, а также имеешь право оспорить решение и исправить свои личные данные, если они неверны или неточны.

Право на подачу **возражения**

- Если твои данные были опубликованы (например, в социальных сетях или в прессе), и это наносит ущерб твоим правам и свободам, ты имеешь право подать возражение против заявителя или автора. Если заявитель не ответит на твое возражение в течение одного месяца или оно не будет удовлетворительным, ты можешь обратиться в инспекцию по защите данных. Ты также можешь обратиться за консультацией в Центр по правам человека.
- Помимо обращения к издателю данных, ты также можешь сообщить об этом через кнопку уведомления на платформе социальных сетей. Если и это не дает результата, можно обратиться в суд против заявителя.
- Если ты возражаешь против обработки персональных данных или собираешься обжаловать ее, ты имеешь право потребовать ограничения обработки персональных данных.
- Если с помощью твоих данных был создан фальшивый аккаунт, сообщи о краже личных данных в полицию здесь: https://cyber.politsei.ee/.

Для **защиты** своих прав ты имеешь право либо напрямую обратиться с ходатайством к обработчику данных (например, почтальону или платформе социальных сетей), либо подать жалобу в инспекцию по защите данных, либо обратиться в суд для защиты своих прав. Если у тебя возникли проблемы или вопросы, связанные с защитой данных или конфиденциальностью, обратись к нам за бесплатной консультацией: **info@humanrights.ee**

Для получения консультации по защите данных обратись к нам со своим вопросом или проблемой:

info@humanrights.ee

3. Кибергигиена

Практикуй здоровые привычки и в сети!

Наряду с оцифровкой мира все больше растет число компьютерных преступлений и кибероперaций. Независимо от того, стоит

ли за ними цель получения финансовой выгоды или политическая или социальная деятельность, любой из нас может стать жертвой подобных махинаций. Но как использовать компьютер, чтобы он не управлял тобой?

Чтобы защитить себя, просмотри следующие пункты.

- **Положения о конфиденциальности**
  Ознакомься с настройками конфиденциальности твоих аккаунтов и положениями, связанными с рекламой. Часто различные приложения и платформы могут быть предустановлены таким образом, чтобы твои данные были видны всем.

- Проверь, комфортно ли тебе, что твои данные используются в настоящее время, и хочешь ли ты решить, какую личную информацию будешь передать платформам и/или третьим лицам.

- Не давай при загрузке некоторых приложений разрешение на **доступ по умолчанию**. Например, нужна ли какой-либо игре информация о твоем местоположении или нужен ли для доступа к твоим контактам фонарик? Конечно, нет!

- **Безопасный** пароль и **двухступенчатая** аутентификация

- Используй безопасные пароли и регулярно обновляй их. Для запоминания паролей можно использовать, например, менеджеры паролей (Keepass, Lastpass).

- Не делись своими паролями ни с кем.

- Двухступенчатая аутентификация значительно повышает безопасность твоих аккаунтов, а большинство приложений и веб-сайтов (FB, Google и т. д.) также позволяют подключить ее.

- **Сначала подумай, потом делись!**

- Когда ты делишься информацией в интернете, всегда думай и учитывай, что ее также можно отправить незнакомым людям или сохранить. Не делись ничем, за что тебе может быть стыдно позже или что ты не хотел бы показывать, например, родителями или начальнику. Всегда спрашивай разрешения людей при публикации их данных, изображений или видео. Удали их данные, если они больше не хотят, чтобы ты хранил их в интернете. Также избегай передачи адресов электронной почты посторонним лицам и при необходимости добавляй адреса в скрытую копию.

- Сделай свой аккаунт приватным и просмотри **список своих друзей**.

- **Сделайте свой Интернет более безопасным!** Подавай пример и сообщай, когда ты видишь ненависть, издевательства или несанкционированный обмен в социальных сетях.

- Храни свой **цифровой мусор** в одном месте и время от времени удаляй старые фотографии, документы и электронные письма.
- При общении с незнакомыми людьми всегда сохраняй **осторожность** и не делись с ними личной контактной информацией или изображениями. В Интернете не все то золото, что блестит, и некоторые «принцы» могут быть сетевыми преступниками.
- Не давай никому **денег в долг** онлайн и береги свою банковскую карту для надежных страниц. Если друг просит у тебя взаймы, узнай у него по другому каналу (например, позвонив), отправил ли он такое письмо и знает ли он, что случилось с его учетной записью.
- Будь внимателен, открывая **ссылки и вложения**.
- Не забывай регулярно проводить на своих устройствах и в приложениях **обновления безопасности**.
- Предпочитай **безопасные** WiFi-**сети**, защищенные паролем.

Утечки данных и нарушения конфиденциальности: будь в курсе о распространенных в Интернете мошеннических схемах!

В Интернете есть правило: если что-то кажется слишком хорошим, чтобы быть правдой, это, вероятно, не так. Целью заманчивого мошеннической схемы может быть зарабатывание денег или захват аккаунта пользователя или компьютера. Это может произойти через электронную почту, социальные сети, веб-страницы или чаты. **Будь бдительным и не нажимай, не задумываясь, потому что каждый щелчок имеет последствия.**

Распознавай распространенные мошеннические схемы и защищай себя

Розыгрыши и лотереи

Кому из нас не нужна бесплатная машина или телефон? Реальная цель таких розыгрышей может заключаться как в получении кликов, так и в зарабатывании денег. Для этого используются разные схемы:

1. В различных каналах социальных сетей распространена следующая схема уведомления о выигрыше в лотерею: когда ты начинаешь оформлять выигрыш, необходимо заплатить деньги, чтобы привести документы в порядок или оплатить доставку.

2. Если ты вводишь данные своей банковской карты на подозрительной странице, мошенник может получить данные карты и совершить с ними ряд покупок в интернете.

3. Также распространены розыгрыши, в которых тебе нужно поделиться своим номером телефона и кодом, полученным с помощью СМС, но может случиться так, что ты подключишься к платной службе контента, и вместо выигрыша тебя ждет дорогостоящий счет за телефон.

4. Мошенничества «лайкни и выиграй»: так владелец страницы может легко направлять тебе рекламу и мошеннические схемы напрямую.

Что делать?

Мы все хотели бы легко зарабатывать деньги, и в Интернете есть множество подобных соблазнов. К сожалению, бесплатных обедов не бывает. Если что-то кажется слишком хорошим, чтобы быть правдой, обычно это неправда!

Не плати деньги в Интернете, чтобы получить выигрыш, и не размещай данные банковской карты на подозрительных страницах. Если ты хочешь что-то купить в Интернете, отдавай предпочтение известным компаниям и безопасным вариантам оплаты – например, используй два разных банковских счета (один связан с платежными картами, а к другому можно получить доступ только через интернет-банк).

Однако если есть желание поучаствовать в «бесплатных» призовых играх, отдавай предпочтение играм известных предпринимателей. Будь внимателен к содержанию лотереи (языковые ошибки, нечеткие условия лотереи, нереалистичные суммы выигрышей или слишком новые страницы), чтобы распознать фальшивую лотерею.

Письмо или сообщение от друга

Если аккаунт друга был взломан, тебе могут отправить сообщение от его имени, чтобы вымогать у тебя деньги или заразить твой аккаунт. Для этого также используются методы манипулирования эмоциями, например, твой друг в беде, и ему срочно нужны деньги. Кроме того, письма могут исходить от незнакомых «принцев», которые предлагают тебе легкий способ заработать деньги.

Что делать?

Если твой друг отправляет тебе неприятное письмо, свяжись с другом другим способом – например, позвони ему и узнай, был ли это он, и знает ли он, что такие письма приходят с его учетной записи. Если друг отправляет ссылку, спроси у друга, почему он ее отправил, прежде чем открывать ссылку. При общении с незнакомыми людьми в Интернете всегда стоит сохранять здравый смысл и рассудительность.

Чарующие знакомства

На сайтах знакомств также есть мошенники, которые могут потратить довольно много времени на построение отношений, но в какой-то момент с ними происходит что-то катастрофическое (например, их жизнь в опасности), и им требуется от тебя немного денег взаймы. Если мошенник также получил интимные изображения или информацию, он может начать шантажировать ими.

Что делать?

Сохраняй осторожность при общении с незнакомыми людьми и не делись с ними личной информацией, даже если они кажутся очень обаятельными и открытыми. Обычно такие преступники вместо этого делятся вещами и данными, отправленными другими жертвами. Определенно не давай взаймы человеку, которого ты в действительности не знаешь.

Клик-магниты

Будь то интересное и привлекающее внимание фальшивое предложение или видео/изображение, при нажатии на него пользователь будет перенаправлен по ссылкам, содержащим вредоносное программное обеспечение, после чего устройство будет заражено вирусами или украдена информация о пользователе или финансовая информация. Твой компьютер может стать медленнее и/или твоя учетная запись может начать рассылать сообщения, чтобы заразить устройства твоих друзей.

Что делать?

Внимательно следи, на какие ссылки нажимаешь, и если что-то кажется подозрительным, то с большой вероятностью найдешь эту информацию и в защищенных каналах.

Предупреждение от IT-поддержки или сотрудника банка

IT-поддержка может уведомить тебя, например, о краже, и попросить тебя сменить пароли с помощью поддельной ссылки, ведущей на какой-либо сайт, напоминающий официальный. При нажатии на ссылку твой компьютер может заразиться вредоносным программным обеспечением, а при обмене паролями преступники могут захватить твою учетную запись. Преступники также могут притвориться сотрудниками банка и попросить пароли для доступа к аккаунту.

Что делать?

Правильные веб-сайты не будут отправлять тебе уведомления с произвольных учетных записей. Также важно знать, что правильный банковский работник при телефонном звонке не попросит твой идентификатор пользователя, личный код и пароли или данные банковской карты (номер карты и код CVC). Банки не регистрируют своих клиентов удаленно через интернет-банк. При получении такого звонка не сообщай свои данные, а если ты по ошибке поделился своими данными, немедленно сообщи об этом в банк (по номеру, полученному на домашней странице), чтобы закрыть свою карту и приостановить платежи.

Для получения консультации по защите данных обратись к нам со своим вопросом или проблемой:

info@humanrights.ee

INIMÕIGUSTE KESKUS

Luminate
Building stronger societies