Приложение 1

Памятка о некоторых способах воздействия и вовлечения украинскими спецслужбами граждан РФ в диверсионно-террористическую деятельность и способах защиты в случае давления и манипулирования со стороны злоумышленников

Расскажем о некоторых правилах бдительности, которые необходимо соблюдать, чтобы не стать жертвой злоумышленников. С целью недопущения совершения противоправных действий террористической направленности разъясняем: если вам, вашим родственникам или близким, поступают звонки от неизвестных лиц, представляющихся сотрудниками правоохранительных органов (ФСБ, полиции, следственного комитета, прокуратуры и т.д.) и звонившие просят поучаствовать в специальной операции (учениях), которые направлены на дестабилизацию работы государства, банковского сектора и т.д. под предлогом проверки работы сотрудников безопасности или правоохранительных органов. Например, изготовить "коктейль Молотова" и кинуть в отдел полиции, военкомат, следственный комитет, прокуратуру и т.д. при этом звонившие будут утверждать, что за данное деяние ответственности никто не понесет, следует помнить, что это не так.

Также могут поступить обещания списания долгов по кредитам (или предложение вознаграждения, возврата похищенных денежных средств) в обмен на осуществление каких-либо действий, дестабилизирующих обстановку в стране и регионе, НЕ ВЕРЬТЕ, Вас обманывают. Помните, оперативно-розыскные мероприятия и следственные действия по телефону не проводятся! Службы безопасности и сотрудники правоохранительных органов никогда не звонят гражданам с сообщениями о необходимости осуществить какие-либо действия в различных целях (перевод денежных средств на нужды больным и раненым в ходе ведения боевых действий, закупку оружия, боеприпасов, взрывных устройств, беспилотных летательных аппаратов на территории Специальной военной операции).

Не переходите по ссылкам, направленным вам в СМС сообщениях и социальных сетях. Не устанавливайте в своих мобильных устройствах программы, которые вас просят установить неизвестные лица. Помните, в соответствии с законодательством Российской Федерации, за совершение противоправных деяний лицо его совершившее несет персональную ответственность. При предложении от неизвестного лица совершить какие-либо противоправные деяния вам следует незамедлительно прервать разговоры со звонившими и обратиться в правоохранительные органы.

Формы и методы деятельности украинских спецслужб по вовлечению граждан Российской Федерации в диверсионно-террористическую деятельность

Обращаем ваше внимание на то, что в настоящее время развернулась тихая, но коварная работа по вербовке россиян и добыче разведданных в сети Telegram. С украинской стороны сейчас делается большая ставка на внутреннюю дестабилизацию России и теракты на нашей территории, в связи с чем схемы вовлечения российских граждан в противоправную деятельность достаточно изощрены.

Схема деятельности врага следующая: сотрудники украинских спецслужб создают в сети Telegram каналы, которые занимаются сбором данных из открытых источников. Пользователи вовлекаются в игровые задания, под прикрытием которых ведётся сбор разведданных и вербовка пользователей.

Пользователь отвечает вроде бы на обычные вопросы и незаметно для себя раскрывает личную информацию. Дальше к работе подключаются психологи, которые, основываясь на полученной информации, уже начинают вербовать человека. Чаще всего такой сбор информации маскируется под обычные квесты, когда пользователям предлагается зайти на какие-то ресурсы, найти определённую информацию, отгадать загадки и собрать ключи и т.д. Игровой формат сбивает пользователей с толку, они думают, что это безобидно, и даже не перепроверяют полученную информацию.

Ещё один распространённый метод разведки и вербовки молодёжи вражескими спецслужбами – так называемые игры ARG. В них задания тоже даются в интернете, а вот игровой платформой становится реальный мир. Несмотря на то, что всё происходящее преподносится как игра, в ней используются реальные номера телефонов, локации, даже вознаграждение победителю. Поначалу игрокам даются простые и как будто безобидные здания – например, сфотографироваться рядом с определённым зданием в городе или объектом оборонного комплекса и передать снимок организаторам. По сути же, так участник неосознанно совершает преступление. После этого манипулировать им можно с помощью угроз и шантажа, а задания становятся, по сути, диверсиями.

Неспроста площадкой для своей деятельности иностранные спецслужбы выбрали Telegram. За годы существования сети у неё сложилась репутация надёжного ресурса с системой шифрования и верификацией каналов. В итоге у людей складывается ложное ощущение безопасности.

Вместе с тем наиболее уязвимая категория пользователей, на которых делают ставку спецслужбы – это подростки. С учётом их интересов легко войти к ним в доверие и воспользоваться гибкостью подростковой психики. Сегодня для этого даже не нужно лично встречаться, как в классических фильмах про шпионов, достаточно создать телеграм-канал с привлекательным для подростков контентом.

Главное правило и защита от подобных манипуляций в интернете – перепроверка достоверности любой получаемой информации. Например, можно поискать информацию о каком-то описываемом в телеграм-канале мероприятии на официальном сайте организатора – действительно ли он проводит ту или иную игру, квест, конкурс и т.д.

Важно! В декабре 2022 года президент РФ Владимир Путин подписал закон о наказании вплоть до пожизненного заключения за создание диверсионных сообществ, финансирование и пропаганду диверсий.

Закон дополняет Уголовный кодекс России тремя новыми статьями: «Содействие диверсионной деятельности» (ст. 281.1 УК), «Прохождение обучения в целях осуществления диверсионной деятельности» (ст. 281.2 УК) и «Организация диверсионного сообщества и участие в нем» (ст. 281.3 УК).

За склонение, вербовку, финансирование или вовлечение в совершение диверсии законом теперь будет предусмотрено наказание от восьми до 15 лет (от десяти до 20 при использовании служебного положения) или пожизненного лишения свободы. Пособничество диверсиям будет наказываться лишением свободы от десяти до 20 лет: в документе оно определяется как умышленное содействие преступлению «советами, указаниями, предоставлением информации, средств или орудий», а также как обещание скрыть преступника.

Законом также предусматривается наказание в виде лишения свободы от 15 до 20 лет либо пожизненного заключения за прохождение обучения для совершения диверсий. Это обучение, согласно документу, представляет собой приобретение знаний «в ходе занятий по физической и психологической подготовке, при изучении способов совершения указанных преступлений, правил обращения с оружием, взрывными устройствами».

Приложение 2

Как украинские спецслужбы вербуют россиян через интернет-квесты

Не всегда игра — это просто игра. Доверчивые пользователи уверены, что играют в игру, а на самом деле помогают врагу. Пока российская армия ведёт боевые действия с противником на реальном фронте, украинские спецслужбы активно «воюют» в виртуальном пространстве. Тихая, но коварная работа по вербовке россиян и добыче разведданных развернулась в защищённой, казалось бы, сети Telegram.

«С украинской стороны сейчас делается большая ставка на внутреннюю дестабилизацию России и теракты на нашей территории, в связи с чем схемы вовлечения российских граждан в противоправную деятельность достаточно изощрены», — сообщают правоохранители. Схема деятельности врага следующая: сотрудники украинских спецслужб создают в сети Telegram каналы, маскирующиеся под OSINT-проекты (англ. Open source intelligence), которые занимаются сбором данных из открытых источников. Пользователи вовлекаются в игровые задания, под прикрытием которых ведётся сбор разведданных о российской «оборонке» и вербовка пользователей.

Напомним: в последнее время правоохранители всё чаще выявляют граждан, занимающихся шпионажем по заданию украинских спецслужб. Подобные действия, напомнили в полиции, попадают под статью 276 УК РФ и предусматривают лишение свободы сроком от 10 до 20 лет.

Как работают иностранные агенты и каким образом пользователи попадают в хитро расставленные ловушки противника? Что за OSINT такой?

Механизм работы украинских спецслужб, на самом деле, давно известный, но, к сожалению, часто не заметный невнимательному или неопытному пользователю. OSINT-проекты – это только один из способов существующей разведдеятельности. Их цель – сбор информации из открытых источников в игровой форме. Пользователь отвечает вроде бы на обычные вопросы и незаметно для себя раскрывает личную информацию. Вражеские аналитики потом всю эту информацию консолидируют и составляют портрет человека. Дальше к работе подключаются психологи, которые, основываясь на полученной информации, уже начинают вербовать человека.

Чаще всего такой сбор информации маскируется под обычные квесты, когда пользователям предлагается зайти на какие-то ресурсы, найти определённую информацию, отгадать загадки и собрать ключи и т.д. Игровой формат сбивает пользователей с толку, они думают, что это безобидно, и даже не перепроверяют полученную информацию. Люди думают, что они выполняют интересные задания, цифровой квест, а на самом деле собирают информацию для недружественных организаций.

Ещё один распространённый метод разведки и вербовки молодёжи вражескими спецслужбами — так называемые игры ARG (Alternative Reality Games). В них задания тоже даются в интернете, а вот игровой платформой становится реальный мир.

Несмотря на то, что всё происходящее преподносится как игра, в ней используются реальные номера телефонов, локации, даже вознаграждение победителю. Всё это очень похоже на городской квест, только участники до конца толком не понимают, в чём участвуют, и не знают ничего об организаторах, поясняют эксперты по цифровой безопасности.

Поначалу игрокам даются простые и как будто безобидные здания – например, сфотографироваться рядом с определённым зданием в городе или объектом оборонного комплекса и передать снимок организаторам. По сути же, так участник неосознанно совершает преступление. После этого манипулировать им можно с помощью угроз и шантажа, а задания становятся, по сути, диверсиями.

Неспроста площадкой для своей деятельности иностранные спецслужбы выбрали Telegram. За годы существования сети у неё сложилась репутация надёжного ресурса с системой шифрования и верификацией каналов. В итоге у людей складывается ложное ощущение безопасности. Каналы для вербовки в Telegram зачастую имеют галочку верификации, которая на самом деле не требует подтверждения. Например, во «Вконтакте» каналу подтвердить свою официальность нужно через портал госуслуг. Для того чтобы получить такую галочку в Telegram, необходимо её просто оплатить.

Интернет помнит всё

К слову, подобные игровые методы сбора информации активно используются и в популярных соцсетях, правда, с более безобидной целью – для настройки таргетированной рекламы. Однако специалисты призывают пользователей быть осмотрительнее и выкладывать даже в соцсетях только тот контент, которым они готовы сейчас или когда-либо в будущем поделиться с миром. В противном случае всё, что хоть раз было оцифровано, может быть использовано против вас.

С точки зрения информационной безопасности использование соцсетей в принципе очень опасно. Если у человека открытый профиль, то по нему определённые люди могут узнать о человеке всё, что им нужно, и воспользоваться этим. Например, человек выкладывает фотографии мест, которые часто посещает, и люди понимают, где его можно встретить. Дальше на связь с ним выходит агент и начинает работу по вербовке».

Если российские сети в последнее время стали более щепетильны в отношении безопасности личной информации пользователей, то запрещённые в России интернет-площадки совершенно точно такой информацией делятся с иностранными спецслужбами.

Акцент на массовость

При всей незатейливости методов украинским спецслужбам всё же удается вовлекать в свою деятельность большое количество пользователей. Как правило, создатели каналов для вербовки работают не над качеством сценария игры, а делают ставку на массовость.

«К примеру, такие каналы охватывают, условно, несколько тысяч человек, из которых клюнут на их приманку, к примеру, 500. То есть, так или иначе, они в кого-то попадут. Кому-то не хватит внимательности, кто-то не обратит внимание на что-то в описании, кто-то просто будет участвовать, что называется, «по приколу». В итоге из-за широты охвата это будет существенное количество людей, с которыми можно проводить дальнейшие манипуляции с комментариями, DDOS-атаками и так далее», – поясняет эксперт по кибербезопасности.

При этом, возраст целевой аудитории украинских спецслужб может быть разным – от детей 6-7 лет, у которых уже есть свободный доступ к гаджетам, до молодых людей 25-30 лет. Люди более старшего возраст обычно попадают в такие «игры» чаще всего сознательно, при определённых политических взглядах.

Вместе с тем наиболее уязвимая категория пользователей, на которых делают ставку спецслужбы, это подростки. С учётом их интересов легко войти к ним в доверие и воспользоваться гибкостью подростковой психики. Сегодня для этого даже не нужно лично встречаться, как в классических фильмах про шпионов, достаточно создать телеграм-канал с привлекательным для подростков контентом.

Каждый телеграм-канал, который создаётся для вербовки, наполняется контентом, максимально интересным для определённой группы лиц. У подростков сейчас, например, популярны какие-то корейские истории, кейпоп-культура. Естественно, они заходят в этот канал, начинается общение – и собираются данные о пользователях.

А вот обезопасить подростка от такого влияния и манипуляций уже сложнее. Над этим работают специалисты по кибергигиене. Они объясняют, что давать доступ к личным данным можно только тем, кому доверяешь; что нельзя добавлять в друзья незнакомых пользователей, даже если это профиль знаменитости, и т.д. Но важно показывать, как это всё работает на конкретных реальных примерах.

«Здесь очень тонкая грань. Подростки сначала в штыки воспринимают информацию, поэтому важно любую информацию в игровой форме на конкретных кейсах преподносить. То есть надо объяснить механизм, как это работает, только тогда это эффективно», – поясняет эксперт по кибербезопасности.

Как защититься?

Главное правило и защита от подобных манипуляций в интернете – перепроверка достоверности любой получаемой информации. Например, можно поискать информацию о каком-то описываемом в телеграм-канале мероприятия на официальном сайте организатора – действительно ли он проводит ту или иную игру, квест, конкурс и т.д.

Ещё один путь – поискать в других источниках отзывы людей о конкретном телеграм-канале и мероприятиях, которые там описываются. Возможно, кто-то уже сталкивался с этим телеграм-каналом, понял, что его пытались завербовать, и где-то в интернете обсуждал эту ситуацию.

Для защиты личных данных от киберпреступников и вражеских спецслужб тоже есть определённые правила. Прежде всего необходимо всегда контролировать, какую информацию человек выкладывает в интернет. Абсолютно всё, что однажды было оцифровано – фотография, сообщение и т.д., даже после удаления продолжает «жить» в виртуальном пространстве.

Особую опасность, подчёркивает эксперт, представляют мобильные операционные системы – поясняет эксперт по кибербезопасности в них автоматически создаются резервные копии всего содержимого гаджета, которые навсегда сохраняются в «облаках».

Важно также пользоваться надёжными приложениями – поясняет эксперт по кибербезопасности лучше отечественного производства или разработки дружественных стран с поддержкой обновлений. Киберпреступники постоянно изобретают всё новые способы добраться до данных пользователей, а разработчики приложений этим угрозам противодействуют, выпуская обновлённые версии программ.

Из-за санкций разработчики приложений из недружественных государств перестали поддерживать свои продукты – и их стало проще взломать. Соответственно, под угрозой оказались и личные данные пользователей таких приложений.

Ну и, конечно, немаловажно повышать информационную грамотность пользователей. Она, по словам экспертов, сейчас на низком уровне независимо от возраста и уровня образованности пользователей. Делать это необходимо комплексно – с привлечением киберагентов или профильных специалистов силовых ведомств. Тогда одной угрозой безопасности в интернете точно станет меньше, настаивают специалисты.

«Есть такое выражение, что основная угроза информационной безопасности обычно сидит перед монитором. И все системы защиты информационной безопасности в целом настроены на то, чтобы минимизировать человеческое участие в данном процессе», – резюмируют специалисты в области кибербезопасности.