Один из очень эффективных методов социальной инженерии — распространение неверной информации среди других людей. В отличие от расхождений во мнениях, дезинформация содержит фактические ошибки. Обычно она направлена на то, чтобы разделить или запутать разные группы людей. Мы часто сталкиваемся с этим в интернете, когда речь идёт о кампаниях влияния. Это кампании, которые обычно проводятся в социальных сетях и затрагивают политические или социальные вопросы.

Есть задокументированные случаи, когда правительство третьей страны или национальное государство разжигают разногласия между разными группами людей. Это может быть сделано для того, чтобы убедить людей поверить во что-то, что не является правдой, или отвлечь их от чего-то очевидного, что может нанести ущерб этому национальному государству. Это может быть даже не связано с веб-сайтом или местом, которое вы посещаете в интернете. Вместо этого информация может быть представлена в виде рекламы, которую вы видите.

А социальные сети — идеальная площадка для распространения дезинформации. Злоумышленники очень умело используют социальные сети и доступные им инструменты для создания статей, а затем делятся ими и ставят лайки, чтобы привлечь как можно больше людей.

Вот как обычно происходит процесс распространения дезинформации. Сначала злоумышленник создаёт несколько аккаунтов с фейковыми пользователями. Это не реальные люди. Все эти аккаунты принадлежат злоумышленнику. Теперь злоумышленнику нужно опубликовать эту дезинформацию в интернете. Он использует один из своих фейковых аккаунтов, чтобы создать контент и опубликовать его в социальной сети.

После публикации в интернете на сайтах социальных сетей обычно появляется возможность поставить лайк, поделиться публикацией или подписаться на автора. Это позволяет злоумышленнику распространить сообщение среди большего числа людей. Алгоритмы социальных сетей распознают, когда тот или иной пост получает лайк или когда им делятся, и показывают его другим пользователям. Как только алгоритм покажет пост другим пользователям, его увидят реальные люди, которые поделятся им со своими знакомыми.

И как только эта дезинформация достигнет определённого уровня популярности, СМИ поймут, насколько она популярна, и начнут создавать собственные истории, чтобы публиковать то, что с самого начала было дезинформацией.

Ещё один интересный приём социальной инженерии — использование названий брендов. Это названия компаний, которые вам, вероятно, знакомы, например Coca-Cola и McDonald’s. Эти бренды мгновенно узнаваемы большинством людей. Поэтому злоумышленники создают сотни или даже тысячи сайтов с таким названием. Затем Google индексирует эти сайты, и они попадают в поисковую систему Google. Если кто-

то будет искать эти бренды в Google, он вполне может попасть на один из таких поддельных сайтов.

Возможно, вы даже сталкивались с этим, когда искали что-то в Google и думали, что переходите на легальный сайт, но при посещении сайта получали всплывающее сообщение или изображение, на котором говорилось, что вы выиграли, что есть специальное предложение и что вам нужно скачать какое-то программное обеспечение. Очевидно, что это программное обеспечение не является легальным. Вероятно, оно содержит вредоносное ПО, и теперь ваш компьютер заражён. Оно будет показывать рекламу. Оно может отслеживать, на какие сайты вы заходите. Или же злоумышленник может получить доступ к данным, которые были украдены с вашего компьютера.