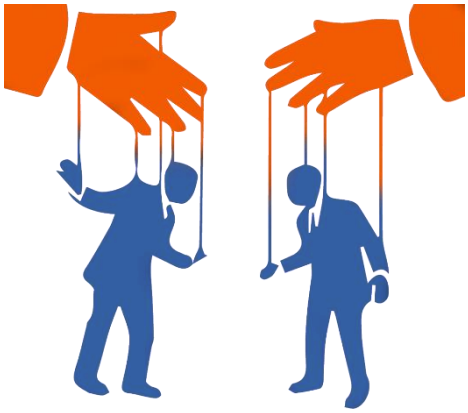

Пять факторов успеха взлома человека

Можно использовать новейшие и самые совершенные технические и программные средства обеспечения безопасности. Но все они будут почти бесполезны, если вы сами даёте злоумышленнику то, что ему нужно. Ибо «ломают» не компьютеры, телефоны и прочие «системы» - в конечном счёте «ломают» вас, их пользователя. Современный злоумышленник, работающий «по-крупному», давно уже не хакер-одиночка, впопыхах освоивший сетевой сканер – сегодня это уже член хорошо организованной группы, который, будучи отлично подкованным техническим специалистом, ещё и прекрасный психолог. Почти все нанёсшие максимальный ущерб (а значит, наоборот, принёсшие максимальную выгоду хакерам) кибератаки начинались со «взлома человека» - с поиска слабых мест в умах и поведенческих привычках обычных пользователей (или конкретного пользователя-жертвы). После того, как такое слабое место найдено, дальше уже, как говорится, дело техники.

Ниже 5 самых распространённых причин, которые ещё долго будут приносить злорадное упоение наживой всевозможных сортов киберпреступникам:

1. **Чрезмерная самоуверенность.** «У меня никогда не крали деньги, а потому никогда и не украдут!». Субъективное, опрометчивое суждение. Подобная точка зрения не должна закрывать вам глаза на реальность угроз и, как следствие, не должна служить основанием неприменения средств защиты – например, того же антивредоносного ПО. Ибо всё когда-то бывает первый раз. Современные вредоносы весьма хитры и могут никак не проявлять себя до поры до времени. Но как только вы воспользуетесь онлайн-банком, ваши деньги «утекут» за секунды.
2. **«Не видеть за деревьями леса»** – давний фразеологизм, означающий потерю главного меж второстепенных частностей. Много информации – не всегда хорошо. В современном океане информации часто чем больше вы узнаёте, тем сложнее становится разобраться в сути проблемы. Вы «теряете фокус» и принимаете неверное решение, подвергая себя рискам.
   Применительно к безопасности это, в частности, означает, что наибольшую пользу приносят только те методы защиты, которые «закрывают» наибольшие именно ваши риски. Любому пользователю необходимо определить какие именно угрозы могут нанести ему наибольший ущерб (а не каких угроз он боится больше всего – чаще всего они не обязательно являются и наиболее опасными!) и использовать адекватные им средства защиты.
3. **Инертность мышления и, как следствие, поведения.** Вы привыкли годами думать определённым образом, потому не успеваете перестроить собственную систему мнений в соответствии с уже изменившимися условиями, в которых вы оказались. 20 лет назад антивирус был единственным средством защиты от вирусов и прочих виртуальных бед. Если вы так же думаете и сейчас – вы в опасности. Сегодня, чтобы чувствовать себя в безопасности (заметьте, мы не пишем «быть в безопасности»!), поневоле приходится хотя бы в общих чертах разбираться с различными поначалу малопонятными вещами вроде «фаервола», «двухфакторной аутентификации» и прочим.
4. **То, что вспоминается проще, кажется более правильным.** Некоторые ещё используют термин «эвристика доступности». Иными словами, в процессе принятия решений данные, которые более доступны (легче вспоминаются, более «свежие», имеют большую эмоциональную окраску), имеют больший вес, чем те, которые вспоминаются с трудом. Это потенциально ведёт к принятию неверных решений: если ваши друзья не пользуются антивирусом и их никогда не «ломали», из этого не следует, что антивирусом не надо пользоваться вообще – есть множество людей, которые серьёзно пострадали от вирусов, но вы о них просто не знаете (или не помните).
5. **Фатализм.** «Что я могу сделать против всех этих организованных и изощрённых туч хакеров? Чему быть - того не миновать!» - говорите вы и не делаете ничего, то есть не применяете никаких средств защиты, полагая, что всё равно всё это бесполезно. Это неверно: игнорируя проблему, вы, очевидно, её не решаете. Между тем, правильное применение современных средств защиты от киберугроз существенно снижает риски стать их жертвой. Да, где-то придётся немного «поизучать вопрос», но в абсолютном большинстве случаев оно того стоит, ибо «цена вопроса» (размер ущерба) намного выше.

Во многом именно на этих моделях мышления и поведения основаны столь часто вспоминаемые нами в наших статьях методы социальной инженерии. В совокупности с нехваткой времени и недостатком знаний у пользователей их использование даёт злоумышленникам большие возможности в реализации своих преступных замыслов.

Главное, что можно и нужно им противопоставить – вдумчивое использование «высоких технологий» и трезвая оценка рисков.