Сериал «Мистер Робот» - это история молодого программиста Эллиота, страдающего социофобией и решившего, что единственный приемлемый для него способ взаимодействия с людьми — это профессия хакера. Данный сериал показывает, как устроен мир информационной безопасности изнутри и насколько мы уязвимы для кибератак.

В своей презентации я хочу показать одну из угроз показанных в данном сериале, правовые нормы, и способы предотвращение данной угрозы.

**Используйте надежные пароли и метод двухфакторной аутентификации.**

Эллиот взламывает аккаунты и получает доступ к информации знакомых и незнакомых легким движением руки — точнее, используя метод брутфорса, когда программа перебирает все возможные комбинации символов или паролей из готовых словарей, пока не найдет подходящую, или его более упрощенный вариант — словарную атаку. Чем более популярна и незамысловата комбинация символов и слов, тем быстрее программа ее обнаружит.

В пилотной серии нам показывают, как Эллиот взламывает аккаунт своего психотерапевта Кристы, пароль которой — Dylan\_2791 — «любимый певец и год рождения наоборот». Догадливому Эллиоту достаточно знать о человеке совсем немного или использовать открытую информацию из его соцсетей.

Что уж говорить про взлом аккаунтов Олли Паркера, его коллеги, пароль которого — «123456Seven» (что особенно комично, ведь Олли работает в сфере кибербезопасности). Взломав один аккаунт, Эллиот легко получает доступ ко всем другим — ведь в Интернете все связано.

Но в одном из эпизодов второго сезона уже к почте самого Эллиота кто-то получает доступ. Герой видит, что в его ящик заходят в разное время и с разных неизвестных ему компьютеров, хотя он постоянно меняет пароль.

**Правовые нормы нарушения**

УК РФ Статья 272. Неправомерный доступ к компьютерной информации

Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

УК РФ Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

Наказывается штрафом в размере до восьмидесяти тысяч рублей или в размере заработной платы или иного дохода осужденного за период до шести месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года.

УК РФ Статья 137. Нарушение неприкосновенности частной жизни

Наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательными работами на срок до трехсот шестидесяти часов, либо исправительными работами на срок до одного года, либо принудительными работами на срок до двух лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового

**Как избежать данной угрозы**

Ян Ширмер, старший аналитик Avast Software, советует всегда создавать сложный, произвольный и уникальный пароль для каждой вашей учетной записи в Интернете. Самый лучший способ запоминания таких сложных паролей — использовать менеджер паролей. Хорошие пароли должны состоять из восьми и более символов, включать цифры, прописные и строчные буквы, знаки. Не используйте какую-либо личную информацию, которую легко найти в сети.

Я рекомендую использовать метод двухфакторной аутентификации. Такая система проверки подлинности просит пользователя ввести еще один код, помимо логина и пароля. Код обычно отправляется на мобильный телефон или генерируется с помощью приложения. Если пользователь на самом деле не пытается войти в свою учетную запись, он получит уведомление его о том, что кто-то другой пытается взломать его аккаунт. Однако, следует отметить, что существуют мобильные вирусы, созданные специально для кражи одноразовых паролей с целью получения доступа к банковским счетам жертвы.

В заключение хочу сказать, не распространяйте личную информацию в интернете, делайте надежные пароли, следите через какие устройства вы заходите в свои аккаунты и изучайте информационную безопасность виды киберугроз. Помните: все, чем вы делитесь, может увидеть кто угодно и использовать против вас.

Соблюдая базовые правила информационной безопасности, можно избежать большое количество киберопасностей.