Киберпреступность

ГБПОУ МО “Чеховский техникум”
Кармилов Артём СА 22/2
Руководитель: Биккулова Оксана Ивановна

Актуальность исследования

Выбранная мной тема интересна своей актуальностью. В наше время, в век информации, СМИ и интернета, эта тема как нельзя кстати. Смотря фильмы, сериалы, мы задаемся вопросом, а все ли так, как показано на экране? Все ли настолько плохо или настолько хорошо? Стоит ли боятся киберпреступлений нам - обычным людям?

Социологические опросы в разных странах, показали, что киберпреступность занимает одно из главных мест среди проблем, которые тревожат людей

Цель работы:

Изучить проблемы развития киберпреступности в мире и России и найти способы ее профилактики.

Задачи:

- Изучить понятие киберпреступность
- Рассмотреть виды киберпреступности
- Найти примеры киберпреступлений в мире
- Дать рекомендации противостояния хакерам в домашних условиях

Гипотеза:

Киберпреступность может перерасти в более глобальную проблему и стать серьёзней бытовых преступлений

Понятие киберпреступности

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. Большинство (но не все) киберпреступления совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги.

История киберпреступлений

История киберпреступлений - это новейшая история, которая касается всех нас. В настоящее время проблема киберпреступности переросла в масштабы мирового сообщества.

Небольшая хронология:

1971 — Джон Дрейнер считается первым телефонным хакером. Однажды он обнаруживает, что в качестве подарка в коробки с кукурузными хлопьями Cap'n Crunch Cereal кладут игрушечный свисток, который издает звук, аналогичный телефонному гудку междугородней связи. Это совпадение позволило ему создать устройство "Blue box"для бесплатных телефонных звонков.

1997 – ФБР сообщает, что более 85% американских компаний подвергаются хакерским атакам, и большинство из атак остаются незамеченными.

2007 – Ущерб от хакерских атак, кражи данных и воздействия вредоносных вирусов резко возрастает. Количество украденных баз данных и учетных записей с зараженных устройств исчисляется миллионами, а размер причиненного ущерба — миллиардами долларов. Китайское правительство обвиняет США в организации хакерских атак.

Виды киберпреступлений

- Фишинг
- Сваттинг
- Кардинг
- DDoS-Атаки
- Кража онлайн-личности
- Распространение запрещенного/незаконного контента

Фишинг

Фишинг — это мошенническая техника, которая используется для кражи личных данных (например, логина и пароля от электронной почты, номера телефона или данных банковской карты).

Сваттинг

Сва́тинг или сва́ттинг (от английской аббревиатуры SWAT) — тактика домогательства, которая заключается во введении полиции в заблуждение (например, путем мистификации, направленной против диспетчера соответствующей спасательной службы) так, чтобы по адресу другого лица выехала штурмовая полицейская группа. Это делается с помощью фальшивых сообщений о серьёзных правонарушениях, такие как закладки бомбы, убийство, захват заложников или другие подобные инциденты.

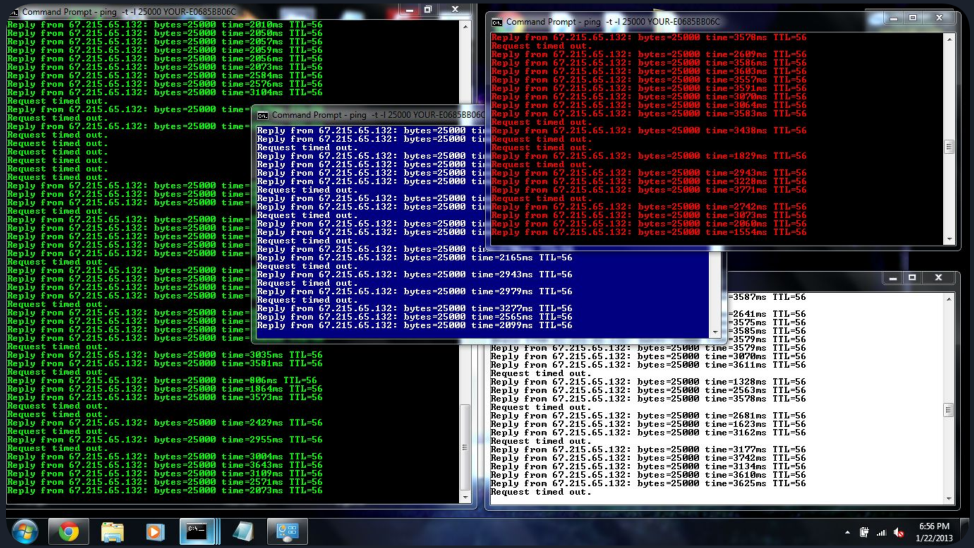
Кардинг

Кардинг — вид мошенничества, при котором хакеры совершают операцию с использованием платежной карты без участия ее владельца.

Один из способов получить доступ к карте — взломать интернет-магазин, где пользователи совершают онлайн-покупки.

DDoS-атаки

DDoS атака — это действия злоумышленников, направленные на нарушение работоспособности инфраструктуры компании и клиентских сервисов. Злоумышленники искусственно создают лавинообразный рост запросов к онлайн-ресурсу, чтобы увеличить на него нагрузку и вывести его из строя.



Кража онлайн-личности

Кража личности (Похищение цифровой личности) (англ. Identity theft) — преступление, при котором незаконно используются персональные данные человека для получения материальной выгоды.

Распространение запрещенного/незаконного контента

Во внесудебном порядке принимаются решения о блокировке следующей информации:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

Пример киберпреступления в мире

Злоумышленники не могли оставить без внимания пандемию. Киберпреступники распространяют сообщения с вредоносными ссылками от имени ВОЗ, создают фейковые благотворительные акции (например, на лечение китайских детей из неблагополучных семей), продвигают несуществующие магазины по продаже масок и антисептиков. Последняя из махинаций только за февраль 2020 года принесла злоумышленникам более 1 млн долл. И это в одной Великобритании (сообщение Sky News).

Как бороться с киберпреступлениями в повседневной жизни

1. К своей основной карте в вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее.

2. Регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций.

3. Храните номер карточки и ПИН-коды в тайне. Запомните и сотрите/заклейте CVC-код

4. Используйте виртуальные карты, которые сейчас предоставляют платежные системы.

5. Поставьте лимит на сумму списаний или перевода в личном кабинете банка.

6. Будьте осмотрительны в отношении писем со вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно.

Информация бралась из:

- https://ru.wikipedia.org/wiki
- Конституция РФ
- Яндекс Дзен

Спасибо за внимание!