Акция «Безопасность в цифровом мире»

Как защитить себя от киберпреступности

Выполнил: Терентьев Михаил Константинович ученик 8 класса Руководитель: Кянжина Татьяна Георгиевна, учитель: информатики ГБОУ СОШ с.Сколково

Сколково, 2025 г.

Киберпреступность — это преступления связаны с использованием технологий для совершения мошеннических действий, кражи личных данных, взлома баз данных, распространения компьютерных вирусов, обмана. Киберпреступники используют уязвимости в компьютерных системах и сетях для получения несанкционированного доступа, кражи конфиденциальной информации, нарушения работы служб и нанесения финансового или репутационного ущерба.

Основные виды

Фишинг

При таком виде атаки хакеры отправляют пользователям письма с зараженными вложениями или ссылками поддельных сайтов, чтобы получить доступ к их учетным записям или компьютеру.

Кража онлайн-личности

Появляется в случаях, когда преступник получает доступ к данным человека, чтобы украсть деньги, провернуть мошеннические махинации от лица жертвы.

DDoS-атаки

Они используются для того, чтобы одновременно направить на требуемый сайт огромное количество запросов из различных устройств, в конечном итоге перегрузить сайт огромным объемом трафика и привести к его отключению от сети.

Gauss, 2012 год

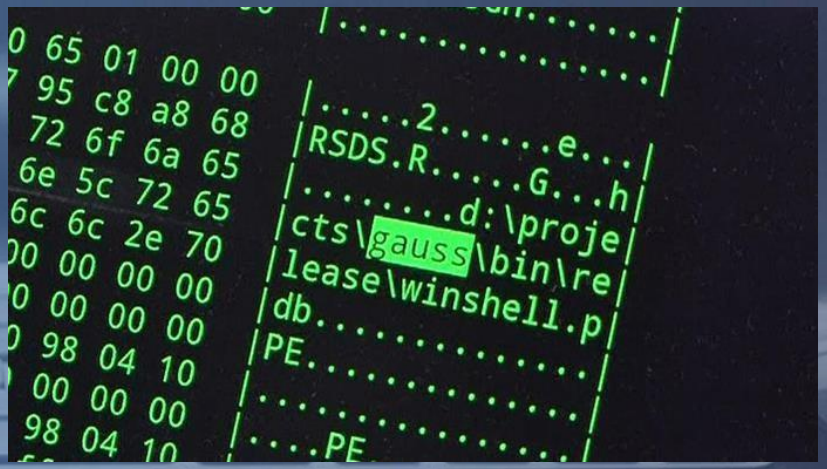
Этот вирус — банковский троян, крадущий финансовую информацию с поражённых ПК — был создан американскими и израильскими хакерами, работавшими в тандеме. В 2012 году, когда Gauss ударил по банкам Ливии, Израиля и Палестины, его причисляли к кибероружию. Главной задачей кибератаки, как выяснилось позже, была проверка информации о возможной тайной поддержке ливанскими банками террористов.

Взлом Facebook в 2020г

Самая громкая утечка данных из соцсети

В марте 2020 года британская компания Comparitech сообщила об утечке данных более 267 млн пользователей Facebook. Большая часть из них принадлежит американцам. Их могли использовать для рассылки фишинговых ссылок.

В августе 2020 года эксперты из компании DarkNet Data Leakage & Breach Intelligence (DLBI) обнаружили в Сети персональные данные 150 млн пользователей Facebook, Instagram и LinkedIn. На этот раз данные похитили с сервера в США, который
принадлежит китайской компании Shenzhen Benniao Social Technology
Она продает рекламу и продвижение в соцсетях



ВЫВОДЫ

Вредоносные программы становятся все более и более мощными, а способы атак постоянно совершенствуются. Атаки все чаще становятся направленными и скоординированными, использующими различные способы заражения.

Я провел опрос среди своих одноклассников и смог узнать много полезной информации.

Диаграмма 1. Данные об осведомленности понятия киберпреступности

На вопрос: что такое киберпреступность смогли верно ответить 41%, затруднения при ответе испытали 10%, не могли ответить на этот вопрос 49%

Диаграмма 2. Анализ жертв киберпреступлений

Часто жертвами киберпреступности становились 15% учащихся, редко - половина (52%), никогда - 33%

Диаграмма 3. Анализ видов киберпреступлений, с которыми сталкивались школьники

Сталкивались с видами киберпреступлений: ложные предложения товаров, услуг, сообщений о поражении вирусом ПК (17%), распространение недостоверной информации (10%), массовой рассылки электронных писем (спама) (23%), распространения вредоносных программ (вирусов) (17%), мошенничества с платежными картами (7%), мошенничество с помощью услуг мобильной связи, телефонными звонками (16%), распространения порнографических материалов (5%), распространения клеветы через Интернет (5%), хищения электронных денег (0%)

Диаграмма 4. Анализ мер защиты, которые применяют учащиеся

Среди необходимых мер защиты от киберпреступлений, которыми чаще всего пользуются школьники – это использование антивирусных программ (44%), использование сложного пароля (19%), аутентификация (21%), внимательное чтение SMS, приходящих по телефону (16%)

Диаграмма 5. Анализ влияния киберпреступления на жизнь человека

Большая часть (57%) считает, что киберпреступность угрожает жизни людей, чаще всего указывая доведение человека до суицида через социальные сети

ВЫВОДЫ:

На основании опроса можно сделать следующие выводы: мои одноклассники сталкивались с той или иной мере со всеми видами киберпреступлений, но больше всего, с мошенничеством с помощью услуг мобильной связи и вредоносным распространение программ, рассылкой электронных писем и ложных предложения товаров и услуг через интернет.

Они знают меры защиты информации, но эти знания недостаточны. Проблема киберпреступлений имеет место для большей части учащихся и они видят в ней угрозу для жизни человека.

Рекомендации для повышения безопасности и защиты от киберпреступности

- Регулярно скачивать обновления для программного обеспечения, часть атак идёт через неисправленные ошибки.
- Настроить межсетевой экран для фильтрации нежелательных входящих соединений.
- Установить качественное антивирусное и антишпионское программное обеспечение.
- Установить спам-фильтр в почтовые программы (например, в Outlook)
- Не открывать писем от незнакомых пользователей.
- Не переходить по ссылкам на известные сайты (соц.сети, банки, интернет-магазины) непосредственно из писем. Очень часто такие письма являются фишинговыми. Придумать (возможно, с помощью специальных генераторов) надёжные не повторяющиеся пароли.
- Хранить несколько резервных копий важных данных.
- Обращать внимание, если знакомые начинают вести себя необычно, игнорировать их просьбы одолжить денег или предоставить другие ресурсы.
- Лучше уточнить подробности по телефону или лично.

С приходом Интернета мы принесли и новую беду. Люди того не понимая, совершают различные операции в интернете, даже не задумываясь о безопасности, и того что их могут взломать или заразить устройство вирусами, воспользоваться личными данными для совершения мошеннических действий.

Надеюсь что материал презентации поможет в какой-то мере защитить себя от киберпреступности.