Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства.

Большинство киберпреступлений совершаются киберпреступниками или хакерами, которые зарабатывают на этом деньги.
Киберпреступная деятельность осуществляется отдельными лицами или организациями.

КИБЕРБЕЗОПАСНОСТЬ

Кибербезопасность — процесс использования мер безопасности для обеспечения конфиденциальности, целостности и доступности данных.

Целью обеспечения кибербезопасности является защита данных.

Борьба с киберпреступностью (belta.by)

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Типы киберпреступлений

- Мошенничество с электронной почтой и интернет-мошенничество
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации)
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)

Виды интернет мошенничества:

- Взлом аккаунтов (Мошенничество с электронной почтой и интернет-мошенничество)
- Фишинг (вишинг) (Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации))
- Травля в сети (кибербуллинг)
- Подозрительные знакомства (груминг)
- Сваттинг (введении аварийно-спасательной службы в заблуждение)
- Нежелательный контент
- Кража финансовых данных или данных банковских карт
- Кража и продажа корпоративных данных
- Кибершантаж (требование денег для предотвращения кибератаки)
- Атаки программ-вымогателей (тип кибершантажа)
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев)
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций)
- Азартные игры
- Трата родительских денег
- Вирусы

Фи́шинг

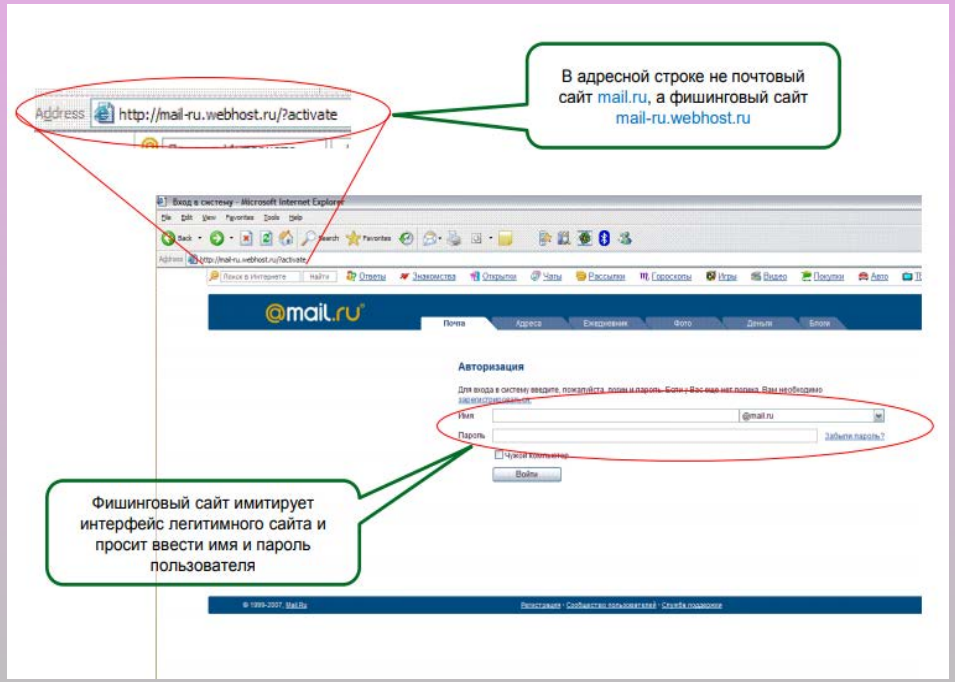
Фи́шинг — вид мошенничества, цель которого является получение конфиденциальных данных для доступа к различным сервисам (электронной почте, странице в социальной сети, интернет-банкингу и т.д.). логинам и паролям Источник

Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

Фишинг: как это работает

www.vkontakte.ru

www. vkomtakte.ru



www.vk.ru

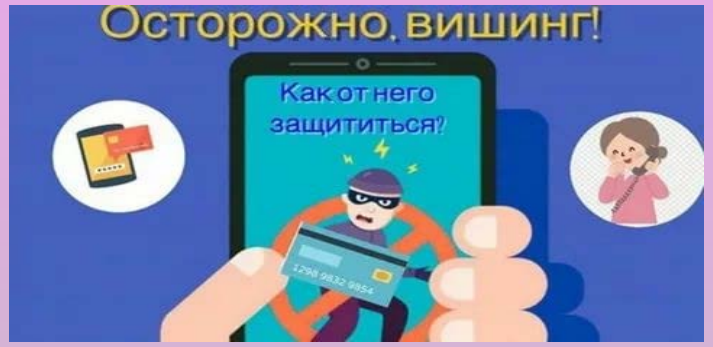
www.vvk.ru

www.paypa1.com

www.paypal.com

Вишинг

Вишинг — один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом / платежной картой.



Сми́шинг

Сми́шинг — вид фишинга через SMS. Мошенники отправляют жертве SMS-сообщение, содержащее ссылку на фишинговый сайт и мотивирующее её войти на этот сайт. Как вариант жертве предлагается отправить в ответном SMS-сообщении конфиденциальную информацию, касающуюся платежных реквизитов или персональных параметров доступа на информационно-платежные ресурсы в сети Интернет.

Скам

СКАМ - Вид интернет-мошенничества, когда злоумышленник сначала втирается к пользователю в доверие, а потом обманывает его.

Чаще всего скамеры знакомятся с жертвой в социальных сетях, на форумах или сайтах знакомств.

Кибератака

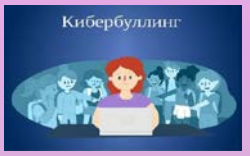
Кибератака — или хакерская атака — это вредоносное вмешательство в информационную систему компании, взлом сайтов и приложений, личных аккаунтов и устройств.

Главные цели — получить выгоду от использования этих данных или шантажа владельцев. Есть целые хакерские группы, которые взламывают сайты, инфраструктуры и сервисы

Кибербуллинг

Кибербуллинг – это вид травли с применением интернет-технологий, включающий оскорбления, угрозы, клевету, компромат и шантаж, с использованием личных сообщений или общественного канала.

Это запугивание, унижение, травля, физический или психологический террор, осуществляемый в виртуальной среде с помощью интернета и мобильного телефона и направленный на то, чтобы вызвать у другого страх и тем самым подчинить его себе.



Если при обычном буллинге используются вербальные и физические акты насилия, в том числе и психологического, то для кибербуллинга нет необходимости личного присутствия.
Все действия совершаются с использованием имейлов, сообщений в меседжерах и соцсетях, а также посредством выкладывания фото и видео-материалов, содержащих губительную для репутации жертвы информацию, в общественную сеть.

Сваттинг

Сватинг – тактика домогательства, которая реализуется посредством направления ложного вызова той или иной службе. Например, люди сообщают о минированиях, преследуя цель устроить неразбериху и панику в конкретном месте. Источник

Цифровая гигиена

Цифровая гигиена – **это** свод правил, следуя которым, человек обеспечивает себе информационную безопасность (не анонимность, а защиту) в сети Интернет.

Как не стать жертвой киберпреступления

- **Регулярно обновляйте ПО и операционную систему, также антивирусное ПО**
- **Используйте сложные пароли**
- **Не открывайте вложения в электронных спам-сообщениях**
- **Не нажимайте на ссылки в электронных спам-сообщениях и не сайтах, которым не доверяете**
- **Не предоставляйте личную информацию, не убедившись в безопасности канала передачи**
- **Свяжитесь напрямую с компанией, если вы получили подозрительный запрос**
- **Внимательно проверяйте адреса веб-сайтов, которые вы посещаете**
- **Внимательно просматривайте свои банковские выписки**

[Киберликбез (mvd.gov.by)]

[Главная причина киберпреступлений - недостаточная цифровая грамотность граждан]

Топ-8 грязных схем

ЗВОНОК ИЗ БАНКА

СБОР ДЕНЕГ НА ЛЕЧЕНИЕ

ПИСЬМО ОТ ДРУГА

ДЕШЕВЫЕ ВЕЩИ

АРЕНДА КВАРТИР

ЗАНЯТОЙ ПОКУПАТЕЛЬ

РОЗЫГРЫШИ И ЛОТЕРЕИ (=ОТДАМ ДАРОМ)

МНЕ ТОЛЬКО ПОЗВОНИТЬ

Базовые правила «общения» с телефонными мошенникам

Основное правило: не сообщайте данные
Перезвоните
Задайте контрольный вопрос
Никаких ссылок
Не переводите деньги
Не перезванивайте
Ошибка перевода: свяжитесь с банком
Проверяйте источники

Не читайте спам-письма

Все эти правила – базовые при общении с мошенниками, но каждый день изобретаются новые способы обмана.

Универсальной защиты от угроз не существует.