УДК 004

КИБЕРМОШЕННИЧЕСТВО

Боярчук В. И., Деде Ю.В.
Научный руководитель: ст. преподаватель Галай Т.А.
Белорусский национальный технический университет

В современном мире наравне с такими преступлениями как мошенничество, кража, убийства, которые происходят непосредственно в реальном мире, на арену серьёзных правонарушений выходит новый вид злодеяний, которые осуществляются в интернете. Быстро набирающий вид имеет совершенно разные вариации и варианты оказания давления на общество. Данная проблема в социуме обрела название кибермошенничество.

Мошенничество в Интернете — это различные методы жульнических действий, исполняемых киберпреступниками в Интернете.

Все идет параллельно: развиваются технологии, появляются новые финансовые продукты, и злоумышленники также совершенствуют свое криминальное ремесло. Количество преступлений в сфере высоких технологий растет на протяжении последних лет. Если углубиться в статистику, то в августе прошлого года в Минской области было зарегистрировано 1100 преступлений этой категории, а в этом году их уже 1400.

Существует множество видов кибермошенничества:

- Вредоносные письма,
- Целевой фишинг,
- SMS-атаки,
- Фейковые приложения,
- Фермы рейтингов,
- Приложения, высасывающие деньги,
- Невидимые скиммеры,
- Скрытые камеры в банкоматах.

Наиболее распространёнными являются следующее методы мошенничества:

1. Электронные письма и SMS-сообщения, отправленные от лица NortonLifeLock, часто пытаются создать ощущение срочности, могут содержать угрозу снять деньги с вашей кредитной карты, если вы не ответите. Они также могут включать предупреждения об истекших настройках антивирусной программы или заражении вашего компьютера. Большинство из них содержат настоятельную просьбу связаться с кем-либо, зайти на поддельный сайт, открыть вложение, позвонить по номеру или предоставить личную информацию или информацию об учетной записи.

2. В сфере технической поддержки. Компании, выдающие себя за поставщиков поддержки программного обеспечения, предлагают услуги поддержки программного обеспечения от имени крупных технологических компаний, чтобы получить доступ к вашей личной информации и использовать ее ненадлежащим образом. Мошенники злоупотребляют вашим доверием, предоставляя ложные сведения о связи с надежными компаниями, и наживаются на страхе, связанном с возможным заражением ваших компьютеров вирусами и вредоносными программами. Многие пользователи тратят сотни долларов на бесполезное программное обеспечение и фиктивные услуги поддержки, что часто приводит к неосознанной загрузке опасного программного обеспечения, которое делает их компьютеры доступными для мошенников.
3. Мошенничество в социальных сетях представляет собой различные публикации в новостных лентах, созданные с целью заставить вас нажать ссылку, которая может содержать вредоносную программу.

Откуда берутся интернет-мошенничества?

Мошенничество в Интернете может принимать форму вредоносного программного обеспечения, такого как вирус или шпионское ПО, которое будет незаметно загружаться на ваш компьютер для кражи ваших паролей и получения доступа к банковским счетам, или будет использовать мошенническую электронную почту и социальную инженерию для вымогательства денег.

Как бороться с интернет-мошенничеством?

Если же говорить о том, как же всё-таки обезопасить себя от данного вида преступления и не стать жертвой злоумышленника, то однозначного варианта ответа на этот вопрос нет. Единственное что сможет вам помочь — это несколько простых правил, которые помогут обезопасить ваши данные. Не верьте никому, кто предлагает вам внезапно много денег; не платите картой, переходя по отправленным вам непонятным ссылкам на почту или в мессенджерах; используйте для оплаты исключительно те сайты, которым лично доверяете или перепроверяйте альтернативно вводя в поисковую систему название сайта для сравнения предложений; не отправляйте никому денег, чтобы потом получить что-то бесплатно; не давайте никому свои пороли либо же пришедшие вам коды.

Литература

1. АО «Лаборатория Касперского»//Спам-фишинг [Электронный ресурс]. – 2023. – Режим доступа: https://www.kaspersky.ru/resource-center/threats/spam-phishing

2. АО «Лаборатория Касперского»//Для вас MMS от банковского трояна [Электронный ресурс]. – 2023. – Режим доступа: https://www.kaspersky.ru/blog/asacub-outbreak/21288/

3. Яноўская А. Кибермошенничество в сети: как не попасть на удочку мошенников? / А. Яноўская // Звязда – 2023. - 20 крас. -С. 3.

ОСОБЕННОСТИ РЕАЛИЗАЦИИ МЕХАНИЗМА «ЕДИНОГО ОКНА» В РАМКАХ ЕВРАЗИЙСКОГО ЭКОНОМИЧЕСКОГО СОЮЗА

Браковская Е.С.
Научный руководитель: преподаватель Жевлакова А.Ю.
Белорусский национальный технический университет

Внедрение концепции «Единого окна» в рамках Евразийского экономического союза является одним из наиболее актуальных и значимых направлений сотрудничества. Это обуславливается тем, что применение данного механизма позволяет упростить и унифицировать процедуры международной торговли, что минимизирует затраты, ускоряет деятельность, как таможенных органов, так и представителей бизнеса. Всё это оказывает благоприятное влияние на конкурентоспособность стран-участниц ЕАЭС.

Согласно Решению Высшего Евразийского экономического совета № 68 «Единое окно» представляет собой механизм взаимодействия между государственными органами, регулирующими внешнеэкономическую деятельность, и участниками ВЭД, который позволяет участникам ВЭД однократно представлять документы в стандартизованном виде через единый пропускной канал для последующего использования [1].

Существуют определённые требования, которые должны быть приняты во внимание при создании «Единого окна» на региональном уровне:

Наличие национального «Единого окна» у каждой страны-участницы ЕАЭС;

Эффективное функционирование и одинаковая доступность каждого национального «Единого окна» в регионе;

Проведение чёткого различия между применением национального и регионального законодательства;

Обеспечение выявления избыточных данных, возникающих в связи с увеличением объема информации и количества процедур, используемых государствами-членами региона;

Определение и доведение до сведения процедур, которые могут быть обработаны региональным «Единым окном»;