Также можно ожидать улучшения системы управления автомобилем и взаимодействия с другими участниками дорожного движения, что повысит уровень безопасности и комфорта при использовании автопилота. В настоящее время выделяют пять уровней задействования автопилота в управлении автомобилем.

В целом, развитие искусственного интеллекта автопилотов автомобилей направлено на создание более умных, эффективных и безопасных систем, которые будут способствовать уменьшению аварий и повышению уровня автомобильного транспорта в целом.

Список используемых источников

1. Autopilot // Wikipedia [Электронный ресурс]. – URL: https://en.wikipedia.org/wiki/Autopilot. - Дата доступа: 16.09.2024.

2. History of self-driving cars // Wikipedia [Электронный ресурс]. – URL: https://en.wikipedia.org/wiki/History_of_self-driving_cars. – Дата доступа: 13.09.2024.

Распространенные виды мошенничества в Беларуси

Жук К.П., Лойко А.И.

Социальная инженерия – это психологическое воздействие на людей, с целью получения конфиденциальной информации для получения финансовой выгоды. Рассмотрим некоторые популярные виды мошенничества, построенные на методах социальной инженерии.

Фишинг – вид мошенничества, который заключается в рассылке сообщений со ссылкой на поддельный сайт, максимально похожий на оригинальный, для завладения паролями, логинами и другой информацией, дающей доступ к финансовым операциям.

Вишинг – метод, построенный на том, что злоумышленники, пользуясь телефонной связью, выбирают определенную роль, вызывающую доверие (сотрудника банка, покупателя и т.д.), использую различные методы, выманивают у жертв конфиденциальную информацию, направляют их к совершению каких-либо действий со своим базовым счетом или банковской картой. Зачастую мошенники направляют звонок не по мобильной/домашней связи, а в мессенджерах, например, по Viber, используя поддельные аккаунты различных банков и представляясь их сотрудниками.

В качестве фото данного аккаунта используют логотипы банков, а ник аккаунта идентичен названию банка. Мошенники рассказывают различные истории: сообщение об оформленном кредите, отмена ошибочного перевода на карту, угроза" блокировки" карточки и другое. По их словам, избежать этих неприятностей можно исключительно сообщив" сотруднику банка" ваши персональные данные.

Фарминг –установка вредоносной программы на девайс жертвы для перенаправления человека на поддельный сайт, не замечая этого.

Дорожное яблоко – этот вид мошенничества завязан на использовании физических носителей (CD, флэш-накопителей) с вредоносной программой. Мошенники оставляют носители в проходимых местах (парковки, столовые, рабочие места сотрудников). Пользователь, найдя этот носитель, для облегчения поиска хозяина открывает его на компьютере и, таким образом, заражает его, если при этом компьютер подключен к большой сети, то заражению подвергается она вся.

Кардинг (от английского carding) – вид мошенничества, построенный на проведении операция с использованием банковской карты или её реквизитов без ведома владельца карты. Злоумышленники, использующие данный метод мошенничества называются кардерами. Чтобы осуществить операции мошенникам нужна информация. Безопасно делится номером банковской карты, так как единственная операция, которую возможно произвести, имея только номер карты– это перевод денежных средств на ваш счет.

Без остальных данных эти цифры не дают доступ к денежным средствам. Но важно помнить, что никогда нельзя сообщать никому комплекс реквизитов, например, номер карты, срок действия и имя владельца.

Так как это позволяет получить доступ к деньгам. Также каждая банковская карта имеет дополнительный код безопасности CVC2 (CVV2, CID). Его сообщать нельзя! Также запрещено сообщать сеансовые пароли или пароль 3-D Secure (секретный код, который приходит вам в смс-сообщениях на телефон при проведении какого-либо платежа).

И, конечно же, нельзя сообщать пин-код. Также нельзя носить его вместе с банковской платежной карточкой. Наше государство обеспечивает защиту интересов и имущественных прав держателей банковских платежных карточек: для них в Беларуси на законодательном уровне установлен принцип” нулевой ответственности“.

Если у вас с карты украли деньги, то вы можете в течение 30 дней обратиться в банк, и деньги вам должны вернуть за 45 дней (в случае, если это произошло в Беларуси), а если операция по списанию денег произошла за пределами нашей страны, то срок возврата удлиняется до 90 дней.

Но следует помнить, что” нулевая ответственность“ действует только при условии, если были соблюдены все правила безопасного использования банковских платежных карточек. Очевидно, что банки всегда находятся в процессе совершенствования своих систем противодействия мошенничеству, для сохранения своей репутации.

В Беларуси найдена новая схема онлайн-мошенничества, основанная на фейковых банковских приложениях. Злоумышленники создают замаскированные программы удаленного доступа под видом настоящих банковских приложений и усиленно распространяют их преимущественно через мессенджеры, представляясь сотрудниками службы поддержки. Они максимально точно воссоздают нужное приложение, добиваясь эффекта полной достоверности. Когда пользователь установит приложение, мошенники получают доступ к

устройству и могут удаленно управлять им, например, отправлять деньги на нужный им счет.

Совсем недавно обрела популярность новая мошенническая схема: злоумышленники подделывают голоса знакомых жертвы. Они очень индивидуально работают с каждым клиентом, а также звонят с белорусского номера, что зачастую для них в новинку. Использую полную открытость некоторых людей в социальных сетях, они получают полный доступ “в семью”.

А дальше на что хватит фантазии: аварии, кражи, срочная взятка, проблемы со здоровьем и так далее. Тяжело отказать родному человеку в тяжелой ситуации, особенно, когда он в слезах и шоке. Это стало возможным из-за стремительного развития возможностей искусственного интеллекта. Помните, что главным тут является возможность положить трубку и перезвонить родственнику на известный вам номер для выяснения всех возможностей.

Также относительно новый способ мошенничества: публикация объявлений о продаже сильно уценённых товаров, например, конфискованных. Публикации обычно размещены в социальных сетях или различных платформах для продажи. Каждый человек, в желании сэкономить, связываются с продавцом, который играет на их чувствах и в спешке выманивает все необходимые для себя данные различными способами: по телефону, через фейковый сайт, используя незнание людей о необходимых мерах безопасности.

Важно всегда проверять правдивость продавца или услуги, помнить, что нельзя предоставлять личные данные ненадежным источникам, хранить бдительность при онлайн-покупках или сделках, которые кажутся слишком хорошими, чтобы быть правдой.

Безопасный счет и помощь в поимке преступника - это ещё одна новая схема злоумышленников. Начинается она со звонка, обычно, через мессенджер. Преступник представляется работником правоохранительных органов и утверждает, что деньги жертвы в опасности: их пытается похитить один из сотрудников банка.

Для усиления эффекта злоумышленники могут поделится фотографией фальшивого удостоверения. Далее идёт призыв к гражданскому долгу, а именно жертву призывают помочь остановить опасного преступника.

Для этого необходимо взять кредит и перечислить средства на якобы безопасный счёт, который, конечно же, тоже участвует в спецоперации по задержанию преступника. Злоумышленники предлагают свою помощь в оформлении кредита и призывают держать всё в тайне, чтобы не сорвать операцию.

Как правило кредит берется на небольшую сумму, для более быстрого оформления. После одобрения деньги нужно перевести на безопасный счет, мошенники утверждают, что так сотрудник не сможет украсть их. Как правильно вы понимаете, после этого жертва деньги уже не увидит.

Теперь немного о средствах защиты от мошенников. Важно всегда проверять подлинность звонка. Не лишним будет перезвонить на номер, который указан на официальном сайте или на обратной стороне вашей карты, чтобы точно убедится, что вы имеете дело не с мошенниками.

В ходе телефонного звонка запрещено сообщать конфиденциальные данные, финансовые и личные данные. Это запрещено делать также при общении по электронной почте или в мессенджерах. Всегда обращайте внимание не оказывается ли на вас давление.

Настоящие сотрудники банков и правоохранительных учреждений не будут на вас давить или торопить, а также запрещать общаться с кем бы то ни было. Также обращайте внимание на возможные манипуляции и подмены понятий в разговоре.

Помните, что официальные лица Республики Беларусь не будут связываться с вами посредством мессенджеров и иностранных номеров. Важно понимать, что пользователь - это слабое звено в системе, поэтому не давайте себя обмануть или сбить с толку это чревато ужасными последствиями. Если же вы все же стали жертвой мошенников незамедлительно обратитесь в банк и в милицию! Берегите себя и своих близких!