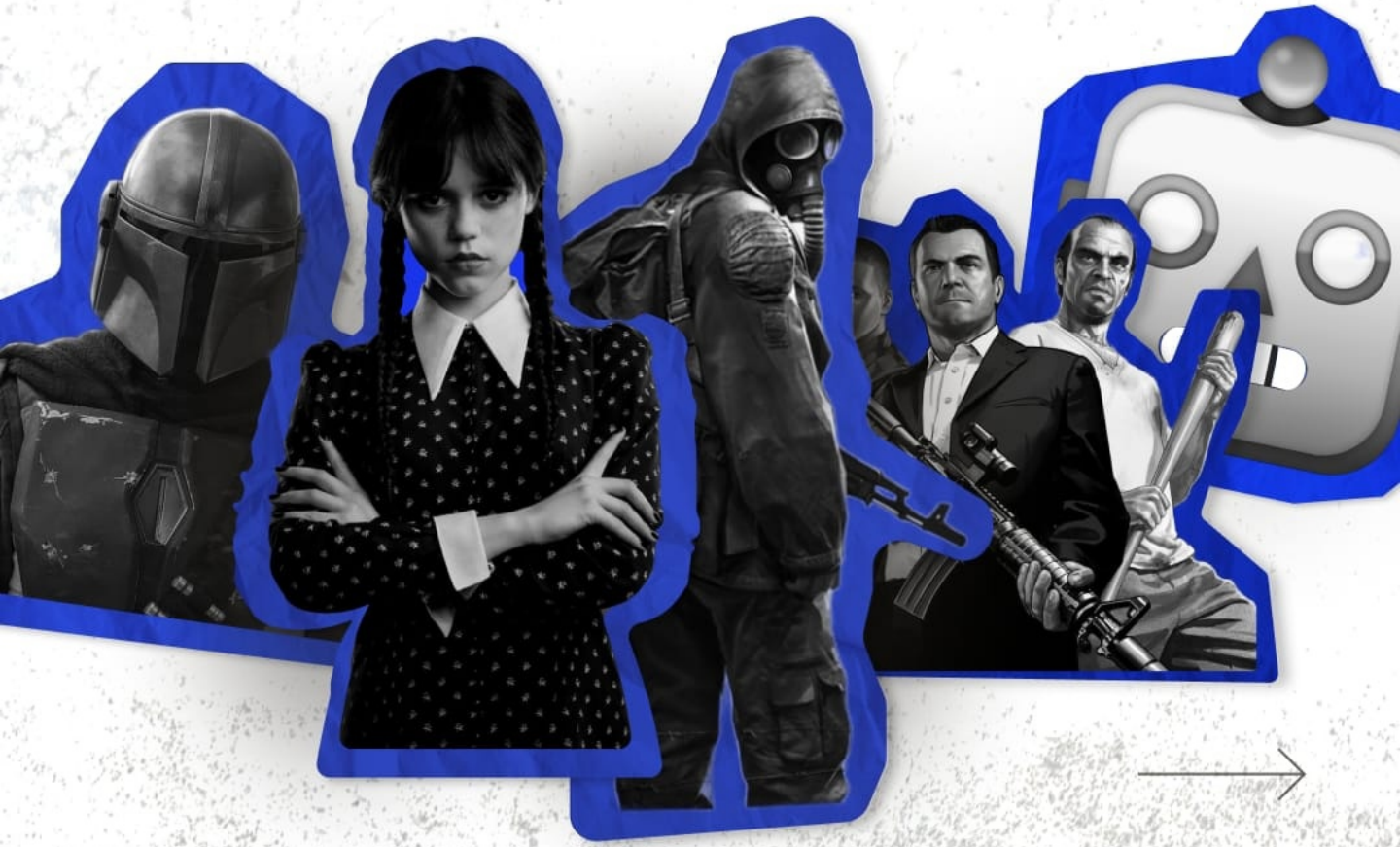
#нцпти_медиабезопасность

5 главных киберугроз 2023 года

и что делать, чтобы не стать их жертвой?



«Скорее переходи по ссылке, чтобы посмотреть новый сезон любимого сериала самым первым!»

Стриминговые платформы каждый год выпускают все больше эксклюзивного контента. 2023 год будет богат на киноновинки. Популярные сериалы и фильмы превращаются в культовые явления, которые влияют на глобальные тренды. В этом году мошенники будут использовать названия стриминговых площадок для создания фишинговых страниц, чтобы украсть персональные данные пользователей.

Один из способов защиты — внимательно смотреть, на какие сайты вы переходите. Для поиска и просмотра контента использовать официальные сайты и не проходить регистрацию на непроверенных площадках.

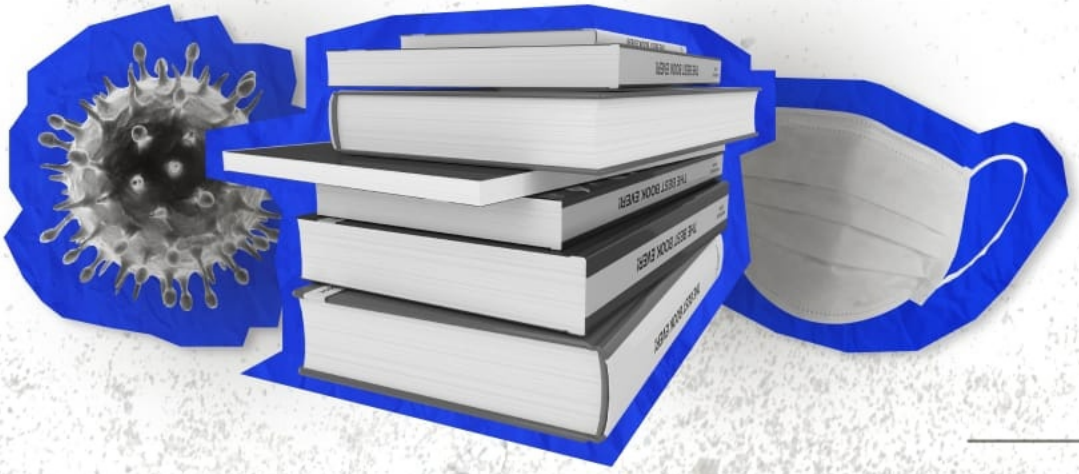
«Следим за здоровьем в реальности, а не в виртуальности»

Тенденция современности — забота о ментальном здоровье. Большое количество приложений для смартфонов помогает пользователю отслеживать свое состояние. Благодаря социальным сетям, в интернете есть масса нашей персональной информации: наши фотографии, интересы, список друзей. Благодаря трекерам ментального здоровья, интернет пополняется информацией и о нашем психическом состоянии. Чем больше пользователей загружают информации, тем больше растет риск утечки подобных персональных данных. А это значит, что мошенники смогут использовать не только данные о номере телефона и имени пользователей, но и информацию о состоянии своих жертв, корректируя мошеннические схемы.

Наш совет — работать с проверенным специалистом. Если возникает необходимость использовать и приложение-трекер, доверяйте только проверенным разработчикам.

«Учиться, учиться и еще раз учиться!»

Пандемия коронавируса во многом помогла цифровизации нашего общества. Появившееся из-за режима самоизоляции свободное время некоторые из нас посвятили прохождению онлайн-курсов. Но мошенники не дремлют. Они создают фишинговые страницы под видом образовательных платформ или площадок для проведения видеоконференций. Соответственно, увеличилось число взломов аккаунтов пользователей, которые регистрируются на образовательных онлайн-площадках.



Учиться в онлайн-формате можно и нужно. Чтобы это было безопасно, внимательно проверяйте организаторов обучения, обращайте внимание на то, какие данные для регистрации вас просят указывать. Помните, что акции и скидки, размещенные на сторонних площадках, не всегда оказываются просто рекламой, иногда это могут мошеннические уловки.

«Меня зовут Александр, я являюсь сотрудником банка, по вашей карте были совершены операции...»

Звонки от мошенников всё еще актуальны, 2023 год может стать для злоумышленников «золотым», благодаря рекордному числу утечек персональных данных.

Для защиты от «колл-центров» рекомендуется установить определитель номера и не отвечать на непроверенные и подозрительные номера.

Помимо этого, ожидается увеличение числа атак с использованием банковских троянов. Клиенты российских банков, попавших под западные санкции, лишились возможности загрузки (а иногда и использования) официальных приложений в маркетплейсах. Им на замену появляются другие приложения, замещающие официальные. Большинство таких приложений пользователи скачивают из непроверенных источников, что грозит взломом мобильных устройств и кражей данных пользователей.

«Принимаем виртуальные деньги к оплате!»

В этом году участится мошенничество в сфере цифровых развлечений. Например, мошенники интересуются виртуальными игровыми валютами. Во многих современных играх есть различные способы монетизации, которые привлекают внимание злоумышленников. Они могут манипулировать своими жертвами и вовлекать их во внутриигровые сделки, чтобы завладеть имуществом других игроков с целью дальнейшей продажи.

Надежный способ защиты — проводить все операции с виртуальной валютой только через официальные площадки.