КИБЕРПСИХОЛОГИЧЕСКИЕ АТАКИ: КОГДА ЦЕЛЬЮ СТАНОВИТСЯ ПСИХИКА

ЮЛДАШЕВА С.З.[1] *- Преподаватель общей педагогики и психологии Джизакского филиала Национального университета Узбекистана*
Шерматов Э.О.[2] *– Студент Джизакского филиала Национального университета Узбекистана направления «Информационные системы и сети (сети и отрасли)»*

В нашем мире, где цифровые технологии все более проникают в различные сферы жизни, киберпреступники и хакеры обнаружили новые способы атаковать не только технические системы, но и человеческую психику. Киберпсихологические атаки становятся все более распространенными и опасными, поскольку они направлены на манипуляцию чувствами, мыслями и поведением людей, а не просто на взлом компьютерных сетей или кражу данных.

Что такое киберпсихологические атаки?

Киберпсихологические атаки представляют собой форму кибератак, которая направлена не только на технические системы, но и на психологические аспекты человеческого поведения. В отличие от традиционных кибератак, которые могут включать в себя взлом систем, кражу данных или распространение вредоносных программ, киберпсихологические атаки целенаправленно используют манипуляции, обман и психологическое давление для достижения своих целей.

Эти атаки могут принимать различные формы, включая социальную инженерию, фишинг, кибермоббинг, кибертравлинг и другие. Основная цель киберпсихологических атак - вызвать эмоциональные или психологические реакции у жертвы с целью получения доступа к конфиденциальной информации, финансовых средств или просто для развлечения на фоне страданий других.

Примером киберпсихологической атаки может быть фишинговая атака, при которой злоумышленник отправляет электронное письмо, выглядящее как официальное сообщение от банка или другой организации, и просит получить доступ к личным данным. Другим примером является кибермоббинг, когда жертва подвергается агрессивным или угрожающим сообщениям или действиям в интернете.

Киберпсихологические атаки представляют серьезную угрозу как для частных лиц, так и для организаций, поскольку они могут привести к утечке конфиденциальной информации, финансовым потерям, а также к

психологическому и эмоциональному стрессу у жертвы. Для защиты от киберпсихологических атак важно быть осведомленным о различных методах атаки, обучать персоналу о правилах безопасности в сети и использовать средства защиты, такие как антивирусное программное обеспечение и фильтры электронной почты.

Примеры киберпсихологических атак

1. Фишинг (Phishing): Это один из наиболее распространенных видов киберпсихологических атак. Злоумышленники отправляют электронные сообщения, которые выглядят как официальные письма от банков, компаний или других организаций, и просят получить конфиденциальную информацию, такую как пароли, номера кредитных карт или социальные страховые номера.

2. Социальная инженерия (Social Engineering): Этот вид атаки включает в себя манипуляцию человеческими факторами для получения доступа к информации или системам. Примерами могут служить звонки по телефону, при которых злоумышленники выдают себя за сотрудников технической поддержки, или ложные представители организаций, которые могут попросить жертву предоставить доступ к системе или информации.

3. Кибермоббинг (Cyberbullying):Этот тип атаки включает в себя целенаправленное оскорбление, угрозы и домогательства через интернет и социальные медиа. Целью может быть вызвать психологические или эмоциональные травмы у жертвы.

4. Кибертравлинг (Cyberstalking): Это атака, при которой злоумышленник наблюдает, преследует и манипулирует жертву через интернет, следя за ее действиями и создавая угрозу для ее безопасности и психологического благополучия.

5. Использование фейковых новостных сообщений: Злоумышленники могут создавать и распространять фейковые новости или информацию в интернете с целью вызвать панику, негативные эмоции или даже изменить общественное мнение о чем-то или кем-то.

Последствия киберпсихологических атак

Киберпсихологические атаки могут иметь широкий спектр последствий, которые могут затронуть как индивидов, так и организации. Вот некоторые из возможных последствий:

1. Эмоциональные и психологические последствия: Жертвы киберпсихологических атак могут испытывать эмоциональный стресс, тревогу, депрессию и чувство беспомощности. Они могут столкнуться с ощущением нарушения личной частной жизни, а также потерей доверия к онлайн-среде.

2. Финансовые потери:В случае успешной атаки, направленной на получение финансовых данных или доступа к банковским счетам, жертвы могут

столкнуться с крупными финансовыми потерями. Кража личной информации также может привести к утрате доступа к финансовым средствам или кредитной истории.

3. Потеря репутации:Если атака включает в себя раскрытие конфиденциальной информации или участие в публичном манипулировании с целью оскорбления или унижения, это может привести к серьезным повреждениям репутации жертвы. Это особенно важно для организаций и общественных лиц.

4. Потеря конфиденциальной информации: Киберпсихологические атаки могут привести к утечке чувствительной и конфиденциальной информации, включая персональные данные, медицинскую и финансовую информацию, бизнес-секреты и другие. Это может повредить конкурентоспособность, нарушить законодательство о конфиденциальности и привести к ущербу репутации.

5. Угроза физической безопасности: В редких случаях киберпсихологические атаки могут представлять физическую угрозу для жертвы, особенно если атака включает в себя манипуляцию системами управления, безопасности или домашними устройствами.

6. Психологическое воздействие на общество: Крупные киберпсихологические атаки, такие как массовое распространение фейковых новостей или манипуляции с общественным мнением, могут иметь широкие социальные последствия, включая усиление напряженности, конфликтов и дезинформации в обществе.

Учитывая эти потенциальные последствия, важно принимать меры для защиты от киберпсихологических атак, включая обучение персонала, использование безопасных практик в сети и регулярное обновление систем защиты информации.

Защита от киберпсихологических атак

Защита от киберпсихологических атак требует комплексного подхода, который включает в себя обучение персонала, использование технологических средств защиты и применение хороших практик в цифровой среде. Вот несколько методов защиты:

1. Обучение и осведомленность: Одним из наиболее важных способов защиты от киберпсихологических атак является обучение персонала о потенциальных угрозах и методах их предотвращения. Это включает в себя обучение о социальной инженерии, фишинге, кибермоббинге и других типах атак, а также о том, как распознавать подозрительные ситуации и действия.

2. Использование антивирусного и антифишингового ПО: Установка и регулярное обновление антивирусного программного обеспечения поможет

обнаруживать и блокировать вредоносные программы, которые могут использоваться в киберпсихологических атаках. Антифишинговое ПО также помогает распознавать подозрительные электронные письма и веб-сайты.

3. Многофакторная аутентификация: Включение многофакторной аутентификации (МФА) повышает уровень безопасности, требуя не только пароль, но и дополнительные формы идентификации, такие как одноразовые коды или биометрические данные. Это делает взлом учетных записей более сложным для злоумышленников.

4. Безопасные пароли и их регулярное обновление: Используйте длинные и сложные пароли для ваших учетных записей, а также регулярно изменяйте их. Пароли должны содержать комбинацию букв, цифр и специальных символов. Используйте менеджеры паролей для хранения и управления паролями.

5. Осмотр веб-сайтов и электронных сообщений: Будьте бдительны при открытии электронных сообщений и переходе по ссылкам в интернете. Проверяйте URL-адреса на подозрительные признаки, такие как опечатки или неправильный домен. Не предоставляйте личную или конфиденциальную информацию через ненадежные источники.

6. Сетевая защита: Используйте механизмы защиты сети, такие как файерволы и виртуальные частные сети (VPN), чтобы защитить свои устройства от несанкционированного доступа и атак из интернета.

7. Регулярные аудиты безопасности: Проводите регулярные проверки безопасности, чтобы выявлять и устранять уязвимости в системах и процедурах безопасности. Это может включать в себя сканирование устройств на наличие вредоносных программ, проверку системы контроля доступа и анализ журналов событий.

Соблюдение этих рекомендаций поможет уменьшить риск киберпсихологических атак и повысить общий уровень безопасности вашей информации и данных.

Заключение

Киберпсихологические атаки представляют собой серьезную угрозу для человеческого благополучия и безопасности в цифровом мире. Понимание и осведомленность об этих атаках являются ключевыми компонентами борьбы с ними. Важно не только защищать технические системы, но и укреплять психологическую стойкость и осознанность у пользователей, чтобы противостоять этому новому виду угроз.