Impact Factor: 9.9 ISSN-L: 2544-980X

Основные Принципы Не Стать Жертвой Киберпреступлений С Учётом Развития Искусственного Интеллекта

Мухамедаминов Азиз Одилжон угли [1], *Anvar Zokhidov* [2]

Аннотация: Интернет оказывает большое влияние на жизнь каждого человека, который им пользуется. С развитием Интернет-технологий и их повсеместном применении развиваются и совершенствуются формы и методы деятельности организаций, а также взаимоотношения производителей и пользователей. Однако возможности Интернета также используются мошенническими организациями для своих целей, привлечения финансовых средств, обмена информацией, планирования и организации мошеннических схем.Современная спам-рассылка распространяется в сотнях тысяч экземпляров всего за несколько десятков минут. Чаще всего спам идет через зараженные вредоносными программами пользовательские компьютеры.

Проблемы с рекламными рассылками (спамом) у частного пользователя начинаются в тот момент, когда его email-адрес попадает в базу данных к спамерам.

Например, Вы получили письмо. В тексте письма есть неуместные знаки препинания, похожие на опечатки: лишние пробелы или обилие заглавных букв (пример — Dear Arsen!!! we CONGR.ATULATE you !!).

Сразу можем определить, что это спам. Таким образом спамеры стараются избежать почтовых фильтров, отсеивающих слова и фразы, характерные для спам-сообщений.

Откуда спамеры узнают ваш адрес?

Проблемы с рекламными рассылками (спамом) начинаются в тот момент, когда email-адрес пользователя попадает в базу данных к спамерам. Например, некоторые интернет-магазины, конференции, форумы и т. п. требуют регистрации с указанием работающей электронной почты. Иногда переданные таким образом адреса попадают к спамерам.

А также спамеры определяют веб-адреса следующими способами:

1. сканируя веб-сайты;
2. сканируя доски объявлений, форумы, чаты, Usenet News и так далее;
3. подбирая «легкие» адреса (nur@, bek@, alex@, info@, sales@, support@) по словарю имен и частых слов;
4. подбирая «короткие» адреса (aa@, ann@, bb@, abc@) простым перебором.

Исходя из этого, можно порекомендовать следующие меры:

Заведите себе два адреса — частный, для переписки (приватный и малоизвестный, который вы никогда не публикуете в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).

[1] UNICON.UZ MChJ инженер 1 категории, Электронная почта: a.muxamedaminov@unicon.uz
[2] Научный сотрудник, Университет Техаса в Далласе (The University of Texas at Dallas) | Член AICA.uz, Электронная почта: anvar.zokhidov@utdallas.edu

1. Адрес для переписки никогда не должен публиковаться в открытом доступе.
2. Адрес для переписки не должен быть легким в запоминании или «красивым». Ваше имя или красивое слово — не подходят.
3. Если нужно сообщить свой приватный адрес (в конференции, на сайте) — делайте это способом, непригодным для автоматического прочтения сборщиком адресов. «student-DOT-собака-mail-точка-ру» — хороший способ. Если речь идет о публикации на сайте, можно опубликовать адрес в виде картинки.
4. Адрес для публикации нужно заранее считать временным. Не стоит его жалеть — вы всегда можете завести новый. Как правило, спам начинает приходить на него через несколько дней после публикации. Поскольку этот адрес могут использовать не только спамеры (туда будет приходить и нормальная почта), стоит его периодически просматривать. Вы можете читать почту, приходящую на него, раз в неделю или раз в месяц.

Правила безопасного общения в социальных сетях

1. Не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма
2. Не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
3. Не размещайте в открытом доступе и не передавайте информацию личного характера.
4. Никогда не отвечайте спамеру. Возможно, ничего плохого не произойдет. Но может случиться и так, что ваш ответ прочитает «робот» и пометит ваш адрес как «живой» — в результате спама будет приходить еще больше. Общаясь в социальных сетях, не следует слепо доверять всем, кто захочет установить с вами контакт. Особенно если в разговоре появляются просьбы, связанные с отправкой SMS на какой-либо номер или отправки внезапно пришедших на телефон кодов.
5. Не пытайтесь воспользоваться ссылкой «отписаться», если вы не уверены, что она сработает. Возможно, вас действительно отпишет данный конкретный рассыльщик. Но при этом ваш адрес могут пометить как действующий… и спама станет больше

Поведение в сети Интернет при использовании онлайн-игр

С каждым годом молодежи в интернете становиться больше, среди них - школьники самые активные пользователи Интернета. Наряду с огромными возможностями, Интернет несет и проблемы. Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но как известно общедоступные Wi-Fi сети не являются безопасными.

Основные советы по безопасному использованию сети Wi-Fi

- Не передавайте свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и другие личные номера.
- Используйте и обновляйте антивирусные программы и firewall. Тем самым вы обезопасите себя от закачки вируса на свое устройство
- При использовании Wi-Fi отключите функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе
- Не используйте публичный WI-FI для передачи личных данных, например, для выхода в социальные сети или в электронную почту
- Используйте только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://».

- В мобильном телефоне отключите функцию «Подключение к Wi-Fi автоматически». Не допускайте автоматического подключения устройства к сетям Wi-Fi без вашего согласия.

Основные советы по безопасному использованию мобильного телефона

- Ничего не является по-настоящему бесплатным. Будьте осторожны, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
- Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
- Необходимо обновлять операционную систему своего смартфона.
- Используйте антивирусные программы для мобильных телефонов.
- Не загружайте приложения от неизвестного источника, они могут содержать вредоносное программное обеспечение. Установку любого приложения необходимо осуществить с официальной маркет площадки мобильного устройства (Google Play Market для смартфонов семейства Android и AppStore для iPhone).
- Периодически проверяйте, какие платные услуги активированы на вашем номере.
- Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете.
- Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.

Основные советы по безопасности игрового аккаунта

- Если другой игрок ведет себя плохо или создает вам неприятности, заблокируйте его в списке игроков.
- Пожалуйтесь администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скриншотов
- Не указывайте личные информации в профайле игры.
- Уважайте других участников по игре.
- Не устанавливайте неофициальные патчи и моды.
- Используйте сложные и разные пароли.

Материалы мошеннического содержания могут не только размещаться на сайтах, но и распространяться посредством электронной почты, в комментариях к статьям, в блогах и т. д. Чтобы распознать подобные ресурсы и обезопасить себя и общества от них, пользователю как никогда раньше потребуется обладать набором цифровых компетенций, включая критическое мышление и информационную грамотность, которые помогут критически анализировать и принять информированное решение.

Будучи вооруженным цифровыми компетенциями, вы сможете не только постоянно повысить свою и защищенность своего окружения онлайн но и внести свой вклад в регулировании вредоносных материалов, содержащих признаки мошенничества.

Новая реальность киберугроз: роль искусственного интеллекта. Искусственный интеллект — усилитель как защиты, так и угроз

Несмотря на то, что перечисленные в этой статье методы по-прежнему эффективны и актуальны, стоит отметить, что масштабы кибератак с использованием искусственного интеллекта резко изменились. Фишинговые и спам-рассылки, упомянутые выше, пострадали больше всего. Игра меняется, и время покажет, что мы получим в итоге. Ранее распознавание фишинговых писем по таким признакам было достаточно надёжным способом защиты: грамматическим ошибкам, неестественному стилю текста, чрезмерному использованию

специальных символов (например: “Уважаемый пользователь,,, Мы рады сообщить...!!!) и странной логике текста.

Однако в настоящее время мошенники используют генеративные модели искусственного интеллекта для создания безупречных фишинговых электронных писем, которые выглядят как настоящие, написанные человеком - даже слишком настоящие.

Такие электронные письма являются:

1. Грамматически правильными;
2. Персонализированными;
3. Корпоративно ориентированными;
4. Оригинальными.

Теперь в дополнение к классическим методам выявления фишинга пользователям приходится осваивать еще больше методов обеспечения безопасности: знание новых форм фишинга, постоянное обучение и самое главное – человеческое мышление. Человеческое мышление всегда было основой любых проблем, и киберугрозы не являются исключением. Читая фишинговое или спам-письмо, нужно стараться не только бегло просмотреть текст, но и понять его. После тщательного прочтения мозг подаст сигналы о том, что там что-то не так. Как уже упоминалось выше, старайтесь обращать внимание на то, насколько реальным является электронное письмо. Если она выглядит слишком реалистично, без единой грамматической ошибки и как будто написана каким-то ученым или поэтом, то это может быть признаком фишинга.

Заключения

Киберпреступность представляет собой динамично развивающееся явление,ставшее одним из ключевых вызовов для современного общества и правоохранительной системы. Многообразие видов киберпреступлений, включающих финансовое мошенничество, нарушение конфиденциальности данных, преступления против несовершеннолетних и атаки на критическую инфраструктуру, создает серьезные проблемы в работе правоохранительных органов. Международное сотрудничество играет ключевую роль в борьбе с транснациональной киберпреступностью, требуя гармонизации законодательств разных стран и развития оперативных механизмов взаимодействия правоохранительных органов. Особое внимание следует уделить предупреждению вовлечения молодежи в киберпреступную деятельность и усилению защищенности информационных систем.

Перспективным направлением является использование искусственного интеллекта в противодействии киберпреступности, однако, его применение требует тщательного правового регулирования, соблюдения этических норм, развития механизмов общественного контроля, систематического повышения квалификации специалистов и внедрения инновационных технологий с учетом соблюдения прав и свобод граждан.

Список литератур

1. Рычаго М.Е. Актуальные вопросы определения киберпространства и отражение киберпреступности в зеркале уголовной статистики / М.Е. Рычаго, Д.Н. Никитин // Пенитенциарное право: юридическая теория и правоприменительная практика. 2023. № 1(35). С. 98–103.
2. Шикула И.Р. Киберпреступность в Российской Федерации: основные методы борьбы и проблемы противодействия / И.Р. Шикула, Е.Н. Куркин // Международный журнал экспериментального образования. 2023. № 1. С. 37–41.
3. Nobles, Calvin & Burton, Sharon & Burrell, Darrell. Cybercrime as a Sustained Business. 2023.