

## Опасности в интернете

преподаватель Собирова Насиба Авазовна

(Наманганский институт иностранных языков имени И.Ибрата)

**Аннотация:** В последнее время огромную популярность получили смс-рассылки или электронные письма с сообщениями о выигрыше автомобиля либо других ценных призов. Почти каждому из нас приходили сообщения с просьбами помочь в трудной ситуации. Мошенников отличает то, что они просят помочь исключительно деньгами. В таких случаях злоумышленники пользуются доверием близких и друзей человека, придумывая самые разные истории. Школьники в этом возрасте наивны и доверчивы, их легко обмануть. В данной работе мы рассмотрели то, как часто дети старших классов попадают на уловки мошенников.

**Ключевые слова:** Безопасность, мошенничество, вирус, социальная сеть, интернет, компьютер.

Интернет настолько проник в нашу жизнь, что что-то заблокировать и запретить совершенно невозможно. Поэтому этот вопрос должен лежать в другой сфере — необходимо формировать культуру работы в интернете, и в этом процессе важна роль преподавателя. В интернете нас могут подстерегать два основных вида угроз: Социальная инженерия. Социальная инженерия — это метод получения необходимого доступа к информации, основанный на особенностях психологии людей. Например, если человеку надавить на жалость, он может выполнить какое-то действие, которое требует от него мошенник. Другой прием — сказать, что «времени нет», тогда человек станет принимать решение быстро и, скорее всего, допустит ошибку. Вирусы и вредоносные программы, которые могут как уничтожить ваши файлы и операционную систему, так и получить доступ к вашей финансовой информации. Самый популярный вид мошенничества — взлом аккаунта кого-то из ваших друзей, когда вам пишет человек с просьбой одолжить денег. Этот вид мошенничества работает, потому что он простой и дешевый. Еще один очень популярный вид жульничества — это сбор средств. Здесь как раз в ход идет социальная инженерия. Вы читаете, и вам с первых строк хочется помочь

и дать денег, вам дают на жалость. Еще один вид мошенничества — выигрыши. Например, это баннер, картинка или плашка якобы от браузера Google, где заявляется, что ваш IP-адрес был выбран в качестве победителя. Понять, что это мошенничество, очень просто, если хотя бы немного понимать, как работает интернет. Во-первых, собрать базу всех IP-адресов невозможно, а даже если такая база есть, то большинство таких адресов будут серверами, а не личными компьютерами. К тому же, Google никогда не проводит лотереи. Платные опросы. Опросы действительно стоят денег, и маркетинговые исследования — это всегда довольно затратно. Спам. Такие письма почти гарантированно содержат в себе вирус. Спам сейчас — примерно 80 % всего потока писем. Вы получаете такое письмо, переходите по ссылке и дальше идет цепная реакция — одна ссылка перенаправляет на другую (а таких перенаправлений может быть сколько угодно много) и рано или поздно вы получите вирус или требование ввести личные данные. Документы и файлы. Кажется, что документы безопасны, но это не так. Вирус — это не только исполняемый файл. В документах могут содержаться макросы. Они потенциально очень опасны. Поэтому если вы не пользуетесь макросами, то вам лучше отключить их исполнение в настройках офисных программ. Как обезопасить себя от угроз? Настройте двухэтапную аутентификацию в соц-сетях. Это спасет вас в случае компрометации вашего пароля. Двухэтапная аутентификация помогает более надежно защитить ваш аккаунт. Если она включена, для входа используются два компонента: то, что знаете только вы (например, пароль) и то, что есть только у вас (например, телефон или электронный ключ). Не открывайте папку спам. Используйте бэкап. Загрузите все свои важные файлы на отдельный диск, который не подключен к интернету. Не пытайтесь заработать на подозрительных схемах. Мыслите и оценивайте информацию критически.

Самые распространенные схемы мошеннических действий в киберпространстве:

- Двойники интернет-магазинов. Невероятно дешевые товары и горячие предложения за полцены призваны завлечь ничего не подозревающих онлайн-покупателей. Через поисковые системы пользователи переходят по ссылке, проходят регистрацию и вводят информацию о своем банковском счете для завершения покупки. В итоге продавец получает оплату и пропадает или присылает совершенно иной товар. Нужно всегда проверять адресную строку в браузере. Она должна начинаться с "https" (безопасный протокол передачи данных), это означает, что ресурс имеет защищенное (шифрованное) соединение, хотя и не гарантирует полной безопасности.
  - Копии сервисов интернет-банкинга. Злоумышленники создают сайты-клоны банков. Посредством электронного письма или смс-сообщения приглашают пользователей пройти авторизацию. Невнимательные граждане переходят на фальшивый сайт, регистрируются в личном кабинете, раскрывая логин и пароль для доступа к финансам. Мошенники при получении данных опустошают банковские счета.
  - Фишинговая атака по электронной почте. Рассылка писем с сообщением о выигранном призе или о блокировке счета. Преступники, как правило, просят победителя перевести определенную сумму для получения крупного выигрыша или внести оплату для разблокировки карты.
  - Взлом аккаунтов и рассылка от друзей с целью наживы. Мошенники пишут на почту или в соцсети родственникам и знакомым владельца страницы с просьбой срочно перевести деньги, придумывая различные ситуации.
  - Фальшивые сайты благотворительности, туроператоров или авиакомпаний. Необходимость срочно собрать деньги на лечение больного ребенка или слишком низкие цены на путевки, просьбы перевести деньги на заграничный банковский счет или электронный кошелек, — все эти моменты должны насторожить пользователей.
  - Предложения выгодного заработка. Недобросовестные работодатели предлагают удаленную работу. Но предварительно требуют оплатить организационные нужды. Как только человек переводит деньги, выдуманная организация пропадает с радаров.
- О схемах мошенников много пишут СМИ, предупреждает полиция. Но преступники придумывают новые сценарии для своих жертв.

Мошеннические схемы направлены на совершение транзакции (безналичного перевода) денежных средств на счет преступников.

Куда сообщать о мошенничестве в интернете? Если пользователь понял, что против него совершены мошеннические действия, необходимо немедленно обратиться:

- В службу технической поддержки банка или платежной системы, осуществляющей переводы денежных средств, чтобы заблокировать счет.
- В полицию по месту проживания.

При предоставлении убедительных доказательств сайт заблокируют.

## **Насколько сурово законодательство Узбекистана к интернет-мошенникам? Удаётся ли привлекать их к ответственности?**

В Уголовном кодексе существует статья «Мошенничество». Надо понимать, что поймать опытных мошенников очень сложно, так как чаще всего при выводе средств они используют чужие карты. Но прецеденты уже есть, и это главное.

Необходимо работать над двумя важными вещами.

Первое: повышать финансовую грамотность среди населения. Хотя бы на базовом уровне. Надо обучать простым вещам: не называть PIN-код своей карты, не передавать саму карту незнакомым людям, в том числе кассирам, хранить в секрете одноразовые SMS-коды. Одним словом, относиться к карте ровно так же, как к своему кошельку.

Второе: Правоохранительным органам широко освещать случаи такого рода мошенничества, чтобы дать понять, что в конечном счёте каждого мошенника ждёт заслуженное наказание.

### **Список использованной литературы:**

1. Baqoyev, Navrozjon (2023). O‘ZBEK TILIDAGI “QO‘L” SO‘ZI VA U QATNASHGAN IBORALAR SEMANTIKASI. *Oriental renaissance: Innovative, educational, natural and social sciences*, 3 (2), 414-417.
2. Bakoev, N., & Abdumutalova, M. (2023). YAPON TILIDAGI KANSAI SHEVASI VA O ‘ZIGA XOSLIGI. *Interpretation and researches*, 1(17).
3. Bakoev, N., & Yuldasheva, S. (2023). YAPONIYA TA’LIM TIZIMI. *Interpretation and researches*, 1(17).

4. Bakoev, N., & Ravshanov, S. (2023). YAPON TILIDAGI IYEROGLIFLAR. *Educational Research in Universal Sciences*, 2(16), 84-87.
5. Bakoev, N., & Sheraliyeva, F. (2023). YAPONIYA TURIZM SOHASI VA RIVOJLANISHI. *Interpretation and researches*, 1(18).
1. Bakoev, N. (2024). ONE OF MODERN LANGUAGE TEACHING METHODS IS TASK-BASED LANGUAGE TEACHING (TBLT) DISADVANTAGES AND ITS SOLUTIONS. *Educational Research in Universal Sciences*, 3(4 SPECIAL), 53–57. Retrieved from
2. Шарофиддинов, М. М. (2016). Из истории железной дороги Бухары. *Молодой ученый*, (9), 962-964.
3. Vokhobjonovna, K. S. (2023). PECULIARITIES OF PEDAGOGICAL VIEWS IN THE WORKS OF ISHAQ KHAN IBRAT. *EPRA International Journal of Research and Development (IJRD)*, 8(11), 156-159.
4. Vokhobzhonovna, X. S. (2023). THE EVOLUTION OF THE CONCEPT OF ACADEMIC FREEDOM IN HIGHER EDUCATION INSTITUTIONS. *American Journal Of Social Sciences And Humanity Research*, 3(12), 365-370.
5. Абдухоликова, Н. А. (2022). ЖАМИЯТ АХБОРОТЛАШУВИНИНГ ИЖОБИЙ САЛБИЙ ХУСУСИЯТЛАРИ. *Conferencea*, 125-129.
6. Абдурасулова, У. (2020). О‘QUVCHILARDA MORFOLOGIK KOMPETENTLIKNI RIVOJLANTIRISH. *ИННОВАЦИИ В ПЕДАГОГИКЕ И ПСИХОЛОГИИ*, (SI-2№ 1).
7. Abdurasulova, U. S. (2019). INNOVATIONAL APPROACH TO IMPROVE MORPHOLOGICAL COMPETENCE. *Scientific and Technical Journal of Namangan Institute of Engineering and Technology*, 1(7), 266-270.
8. Mamasodikova, M. (2022). THE CATEGORY OF APPRAISAL IN RUSSIAN ROCK POETRY. *Oriental renaissance: Innovative, educational, natural and social sciences*, 2(6), 130-133.
9. Мамасодикова, М. Ж. (2024). РУССКАЯ РОК-ПОЭЗИЯ КАК ЛИТЕРАТУРНОЕ И ЛИНГВОПОЭТИЧЕСКОЕ ЯВЛЕНИЕ. *World of Scientific news in Science*, 2(1), 403-412.

10. Sobirova Nasiba Avazovna Ta'lim jarayonini raqamlashtirishning metodologik asoslari.  
“Interpretation and researches”/ vol.1, 2023, p. 274-277
11. Собирова, Н. А. (2024). ЦИФРОВИЗАЦИЯ УЧЕБНОГО ПРОЦЕССА. Educational Research in Universal Sciences, 3(4 SPECIAL), 58–62
12. Собирова, Н. (2024). ОПАСНОСТИ КОТОРЫЕ ТАЯТСЯ В ИНТЕРНЕТЕ. Interpretation and researches, 2(24).