DOI: 10.58168/STR2026_258-264
УДК 004.7

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ
INTERNET SAFETY

Ермаков С.А., кандидат филол. наук, доцент кафедры иностранных языков ФГБОУ ВО «Воронежский государственный лесотехнический университет им. Г.Ф. Морозова», Воронеж, Россия.

Павлов Е.С., студент бакалавриата, группа ИС2-241-ОБ, ФГБОУ ВО «Воронежский государственный лесотехнический университет им. Г.Ф. Морозова», Воронеж, Россия.

Ermakov S.A., Candidate of Philological Sciences, Associate Professor of the Department of Foreign Languages, Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia.

Pavlov E.S., bachelor's degree student, group IS2-241-OB, Voronezh State University of Forestry and Technologies named after G.F. Morozov, Voronezh, Russia.

Аннотация: В материале собрана актуальная информация о рисках, подстерегающих пользователей в глобальной сети. Детально разбираются рабочие схемы мошенников - от поддельных писем из банков до вирусов в рекламных баннерах. Объясняется, как распознать обман на разных этапах - при просмотре сайтов, получении сообщений, скачивании файлов. Рассматриваются принципы создания надёжных паролей и настройки двухэтапной защиты. Приводятся примеры из жизни, когда соблюдение простых правил безопасности помогло избежать потери денег и данных. Даются чёткие инструкции по проверке подозрительных ссылок и настройкам приватности в браузерах.

Ключевые слова: мошенничество, фишинг, пароли, аутентификация, безопасность, вирусы, шифрование, конфиденциальность.

Abstract: The material contains up-to-date information about risks that wait for users online. Real fraud schemes are broken down - from fake bank emails to viruses in ads. It explains how to spot scams at different stages - while browsing websites, getting messages, downloading files. The principles of creating strong passwords and setting up two-step verification are examined. Real cases are presented when following basic security rules helped prevent data and money loss. Clear instructions are provided for checking suspicious links and adjusting privacy settings in browsers.

Keywords: fraud, phishing, passwords, authentication, security, viruses, encryption, privacy.

Сложно представить современную жизнь без интернета - мы в нем работаем, общаемся, покупаем и отдыхаем. И как точно подмечено: «интернет стал частью жизни почти каждого человека, и большая часть общения, работы и вообще всего теперь проходит именно там» [1]. Но в этой удобной привычке кроется и главная опасность - мы стали выкладывать в сеть слишком много, даже не задумываясь. Сфоткал что-то, выложил - и все, информация уже ушла в свободное плавание. Не лучше ли остановиться и спросить себя: а что именно я показываю незнакомым людям и зачем?

Удивительно, как много людей попадается на фишинговые письма. А все потому, что, как отмечают эксперты, «фишинговые письма до сих пор остаются одним из самых частых методов обмана, потому что они выглядят правдоподобно и заставляют человека торопиться» [2]. Многие просто не хотят тратить время на проверку: пришло письмо - ну, нажму на ссылку. Хотя если внимательно посмотреть на адрес отправителя или на странные формулировки в тексте, часто все становится понятно. Мы все спешим, и мошенники на этом как раз и играют.

С антивирусами та же история. Да, они помогают, но нельзя просто поставить и забыть. Ведь «антивирусы и защита на устройствах действительно помогают, но если их не обновлять, то толку от них немного» [3]. У многих он просто работает в фоне, а обновления постоянно откладываются. А ведь это не просто надоедливые

уведомления, а реальная защита от новых угроз. Потратить пару минут - и потом не придется разбираться с последствиями.

Бесплатный Wi-Fi в кафе — это, конечно, удобно, но и рискованно. Ведь «проблема с бесплатными Wi-Fi сетями в том, что они открыты для всех, включая тех, кому вообще не стоит туда залезать» [1]. Мало кто задумывается, что сеть может быть поддельной, а все введенные пароли и данные из интернет-банка - перехвачены. Если уж и подключаться к такой сети, то лучше не вводить ничего важного. В таких случаях лучше предпочесть мобильный интернет - хоть и медленнее, но спокойнее.

С детьми в сети отдельная история. Им сложно объяснить, что не все и не всем можно доверять, ведь «дети и подростки в интернете сталкиваются с огромным количеством вещей, которые они ещё не в состоянии правильно оценить» [2]. Они могут отправлять фото или делиться личным просто потому, что не видят в этом риска. Запреты тут не работают - ребенок все равно найдет лазейку. Гораздо полезнее, по-моему, спокойно и по-взрослому объяснять, что к чему, и показывать примеры. Это долгий процесс, но он того стоит.

Многофакторная аутентификация, конечно, иногда раздражает, когда нужно ждать код. Но ее нужно ценить, ведь «многофакторная аутентификация значительно снижает риск взлома аккаунтов, поскольку для входа требуется подтверждение личности через несколько независимых способов» [3]. Это как второй замок на двери. Даже если твой пароль утечет, без этого кода злоумышленник не пролезет. Для почты, банковских приложений и соцсетей - вещь просто необходимая.

Мы сами порой своими руками создаем себе проблемы. Ведь «люди сами нередко выкладывают в соцсети такие вещи, которые могут потом сыграть против них, и даже не замечают этого» [4]. Фотка с пропуском на работе, пост о долгожданной поездке, который кричит всему миру, что квартира пустая... Все это - информация. Не нужно жить в паранойе, но немного фильтровать, что ты публикуешь, никогда не помешает. Иногда стоит просто задать себе вопрос - А кому, кроме близких друзей, это действительно нужно видеть?

Многие почему-то свято верят, что если сервис крупный и известный, то за тебя там всё продумали. Но «иногда пользователи слишком доверяют автоматическим

системам и сайтам, считая, что если сервис известный, то там всё идеально защищено» [5]. Это иллюзия. Даже гиганты IT ошибаются, а уж мошенники только и ждут, чтобы этим воспользоваться. Поэтому всегда, даже когда торопитесь, постарайтесь не тыкать «далее» не глядя, а пробегаться глазами, на что соглашаетесь. Интернет - инструмент, и пользоваться им нужно с включенной головой.

Самый неприятный метод, на мой взгляд, — это когда тебя не взламывают, а просто обманывают. Ведь «мошенники всё чаще используют методы социальной инженерии, когда они не ломают системы, а просто манипулируют человеком, заставляя его самому выдать нужную информацию» [1]. И ведь работает! Потому что кто ж ждет подвоха от вежливого «сотрудника банка», который так убедительно просит «подтвердить данные для безопасности». Для себя нужно уяснить простое правило: настоящие организации никогда не будут спрашивать у тебя пароли, пин-коды или коды из SMS. Если просят — это стопроцентно мошенники.

А эти бесконечные пользовательские соглашения... Кто их вообще читает? А зря, ведь «сайтам и приложениям тоже нельзя полностью доверять, потому что нередко пользователи сами соглашаются на сбор данных, не читая условий» [4]. Мы все виноваты - просто жмем «разрешить», чтобы поскорее начать пользоваться. А потом удивляемся, откуда столько спама или куда утекла личная информация. Потратьте минуту, чтобы зайти в настройки и отключить лишние разрешения - доступ к контактам, геолокации, микрофону без надобности. Это не требует особых знаний, просто чуть больше внимания к тому, что ты делаешь.

С паролями вечная беда. Ведь «у многих людей до сих пор слабые пароли - что-то вроде 12345 или даты рождения - потому что так легче запомнить» [3]. Конечно очевидно, что запоминать кучу сложных комбинаций - то еще мучение. Но для всего самого важного - почты, банка, облака с документами - все-таки нужно придумать что-то серьезное. Помогает метод: беру простую фразу, известную только мне, и заменяю буквы на цифры и символы. Взломщики ведь не вручную подбирают, у них программы, которые простые пароли щелкают за секунды. Так что эти усилия точно того стоят.

Мы стали слишком беспечными к своим старым аккаунтам. Создал где-то профиль лет десять назад, воспользовался пару раз и забыл. А он все висит, и там может быть привязана старая почта или, что хуже, тот же пароль, что и для важных сервисов. Ведь «мошенники всё чаще используют методы социальной инженерии» [1], и такие забытые аккаунты - легкая добыча.

И еще один момент, который многие упускают, — это резервные копии. Казалось бы, какое отношение это имеет к безопасности? Самое прямое. Если тебя взломают, заразили вирусом-шифровальщиком или ты просто потеряешь телефон, все твои фото, документы и переписки могут исчезнуть навсегда. Да, «антивирусы и защита на устройствах действительно помогают» [3], но стопроцентной гарантии не дают. Нужно перекидывать все действительно важное на внешний жесткий диск. Это занимает немного времени, зато потом не придется платить выкуп мошенникам или рыдать над утраченными воспоминаниями. Это как страховка: надеешься, что не пригодится, но она есть.

Часто люди переоценивают свою внимательность. И тут проблема даже не в незнании, а в излишней уверенности, ведь «иногда пользователи слишком доверяют автоматическим системам и сайтам, считая, что если сервис известный, то там всё идеально защищено» [5]. Кажется, что уж я-то точно не попадусь на удочку мошенников, я же человек грамотный. Но именно эта уверенность и расслабляет. Когда видишь знакомый логотип банка или почты, рука сама тянется ввести данные - а это может быть ловко сделанная подделка. Особенно, когда торопишься или устал.

Важно понимать, что безопасность — это процесс, а не разовое действие. Ведь «антивирусы и защита на устройствах действительно помогают, но если их не обновлять, то толку от них немного» [3]. Эта же логика работает и с нашими привычками. Недостаточно один раз поставить антивирус и придумать сложный пароль. Нужно регулярно обновлять программы, проверять настройки приватности, следить за новыми видами мошенничества. Это как уход за машиной - нельзя поменять масло один раз и навсегда.

И самое главное - не стоит паниковать и думать, что все безнадежно. Да, «иногда пользователи слишком доверяют автоматическим системам и сайтам» [5], но, с другой

стороны, не нужно впадать и в другую крайность - полного недоверия. Угроз в интернете много, но это не значит, что нужно вообще отказаться от его использования. Просто нужно выработать полезные цифровые привычки: проверять ссылки перед переходом, не хранить все пароли в одном месте, делать резервные копии важных файлов. Эти простые действия действительно помогают снизить риски.

Еще многие не задумываются, что, даже просто читая новости или смотря видео, мы оставляем след. Ведь «иногда пользователи слишком доверяют автоматическим системам и сайтам» [5], не задумываясь, что нас отслеживают через куки, историю поиска, лайки. Это не значит, что нужно сидеть в интернете в противогазе, но понимать, как работает сбор данных - полезно. Хотя бы чтобы знать, почему вы вдруг везде видите рекламу того, о чем вчера только думали.

И последнее - не стоит пренебрегать простыми советами. Ведь «дети и подростки в интернете сталкиваются с огромным количеством вещей, которые они ещё не в состоянии правильно оценить» [2]. Но и взрослые часто игнорируют базовые правила безопасности. Кажется, что со мной ничего не случится, я же не ребенок. Однако мошенники как раз рассчитывают на эту беспечность. Лучше десять раз перепроверить, чем один раз пожалеть.

В итоге получается, что безопасность в интернете — это про простую внимательность в повседневных вещах. Ведь «иногда пользователи слишком доверяют автоматическим системам и сайтам, считая, что если сервис известный, то там всё идеально защищено» [5]. Не нужно быть экспертом по кибербезопасности, чтобы проверять отправителя подозрительного письма или не подключаться к первому попавшемуся открытому Wi-Fi. Главное - не терять здравый смысл и помнить, что за милой картинкой или срочным сообщением может скрываться ловушка. Если что-то кажется странным - скорее всего, так оно и есть.

СПИСОК ЛИТЕРАТУРЫ

1. Pomoschryadom.ru. Безопасность в Интернете. – URL: https://pomoschryadom.ru/helpful-articles/safety/bezopasnost-v-internete (дата обращения: 24.10.2025).

2. Dgcsssdm.ru. Безопасность в Интернете. – URL: https://dgcsssdm.ru/stati-2/article_post/bezopasnost-v-internete (дата обращения: 24.10.2025).

3. Kaspersky.ru. Что такое интернет-безопасность? – URL: https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security (дата обращения: 24.10.2025).

4. КиберЛенинка. Безопасность в сети Интернет. – URL: https://cyberleninka.ru/article/n/bezopasnost-v-seti-internet (дата обращения: 24.10.2025).

5. ОмПЭК. Безопасность в сети Интернет. – URL: https://www.ompec.ru/about/structura/podrazdelenie/sotsialno-psikhologicheskaya-sluzhba/materialy/?ELEMENT_ID=1603 (дата обращения: 24.10.2025).

REFERENCES

1. Pomoschryadom.ru. - URL: https://pomoschryadom.ru/helpful-articles/safety/bezopasnost-v-internete (Access date: 24.10.2025).

2. Dgcsssdm.ru. - URL: https://dgcsssdm.ru/stati-2/article_post/bezopasnost-v-internete (Access date: 24.10.2025).

3. Kaspersky.ru. - URL: https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security (Access date: 24.10.2025).

4. Cyberleninka.ru. - URL: https://cyberleninka.ru/article/n/bezopasnost-v-seti-internet (Access date: 24.10.2025).

5. Ompec.ru. - URL: https://www.ompec.ru/about/structura/podrazdelenie/sotsialno-psikhologicheskaya-sluzhba/materialy/?ELEMENT_ID=1603 (Access date: 24.10.2025).