Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Демьяненко В.С., Костур О.Г. Цифровая гигиена и личная безопасность в интернете // Академия педагогических идей «Новация». Серия: Студенческий научный вестник. – 2025. – №4 (июнь) – АРТ 7-эл. – 0,2 п.л. - URL: http: //akademnova.ru/page/875550

РУБРИКА: ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.5

Демьяненко Виктория Сергеевна,
студентка 2 курса, Физико-Технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация
e-mail: vdem1716@yandex.ru

Костур Ольга Геннадьевна,
студентка 2 курса, Физико-Технический институт
ФГАОУ ВО «КФУ им. В.И. Вернадского»
г. Симферополь, Российская Федерация
e-mail: olgadance20@gmail.com

ЦИФРОВАЯ ГИГИЕНА И ЛИЧНАЯ БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ

Аннотация: в статье рассматриваются современные схемы кибермошенничества и методы защиты от них с акцентом на уязвимости человеческого фактора. Представлен детальный разбор 20 популярных мошеннических схем, включая звонки от «родственников», фальшивые банковские уведомления и поддельные сайты. Описаны технические и поведенческие меры защиты, такие как двухфакторная аутентификация и критическая проверка информации. Практическая часть включает анализ семейного обсуждения, демонстрирующего эффективность повышения кибериммунитета через информирование. Научная новизна заключается в систематизации схем мошенничества и подходов к их профилактике с учетом психологических аспектов.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Ключевые слова: цифровая гигиена, кибербезопасность, кибермошенничество, социальная инженерия, двухфакторная аутентификация, человеческий фактор, интернет-безопасность.

Demyanenko Victoria
2nd year student, Physics and Technology Institute
FGBOU VO " V.I. Vernadsky Crimean Federal University"
Simferopol, Russian Federation
e-mail: vdem1716@yandex.ru

Kostur Olga
2nd year student, Physics and Technology Institute
FGBOU VO " V.I. Vernadsky Crimean Federal University"
Simferopol, Russian Federation
e-mail: olgadance20@gmail.com

DIGITAL HYGIENE AND PERSONAL SAFETY ON THE INTERNET

Abstract: the article examines modern cyberfraud schemes and methods of protection against them, with a focus on human factor vulnerabilities. A detailed analysis of 20 prevalent fraudulent schemes is presented, including calls from "relatives," fake bank notifications, and counterfeit websites. Technical and behavioral protection measures, such as two-factor authentication and critical information verification, are described. The practical section includes an analysis of a family discussion, demonstrating the effectiveness of enhancing cyber-immunity through awareness. The scientific novelty lies in the systematization of fraud schemes and prevention approaches, considering psychological aspects.

Keywords: digital hygiene, cybersecurity, cyberfraud, social engineering, two-factor authentication, human factor, internet security.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Введение

В условиях стремительного развития цифровых технологий и повсеместного использования интернета вопросы кибербезопасности становятся критически важными. Человек остается наиболее уязвимым звеном в любой системе кибербезопасности, что делает развитие кибериммунитета приоритетной задачей [1]. Целью данной работы является повышение уровня кибериммунитета через детальный разбор современных схем кибермошенничества и методов защиты от них с акцентом на уязвимости человеческого фактора. Актуальность исследования обусловлена ростом числа киберпреступлений, использующих технологии искусственного интеллекта и методы социальной инженерии, а также необходимостью формирования осознанного поведения пользователей в цифровой среде.

Уязвимости человеческого фактора в кибербезопасности

Человек является наиболее уязвимой частью любой системы кибербезопасности. Мошенники эксплуатируют базовые психологические механизмы, такие как страх, доверчивость и поспешность в принятии решений. Одним из слабых мест в защите личных данных является использование четырехзначных кодов для доступа к личным кабинетам, например, в сервисах мобильных операторов, где телефон выступает логином, а пароль — четырехзначным кодом. Это делает такие системы уязвимыми для атак социальной инженерии, усиленных применением искусственного интеллекта, который позволяет создавать правдоподобные сценарии обмана [2].

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Популярные схемы кибермошенничества и методы защиты

Современные кибермошенники используют разнообразные схемы, направленные на манипуляцию пользователями. Ниже приведен разбор 20 популярных схем, характерных для Крыма и других регионов, с рекомендациями по защите:

ДТП с родственником: Мошенники звонят, представляясь родственником, попавшим в аварию, и требуют деньги. Защита: Положить трубку и перезвонить предполагаемой «жертве». Выиграть 10 секунд для осмысления ситуации. Придумать семейный пароль для идентификации подлинных звонков.

Звонок от «начальника»: Используется дипфейк или подмена голоса. Защита: Указать на подозрительность и попросить передать трубку реальному начальнику. Мошенники не смогут поддерживать правдоподобную беседу.

Служба безопасности банка: Утверждают о несанкционированной транзакции. Защита: Спросить, с какой карты и какого банка идет транзакция, сказать: «Блокируйте, завтра получу новую карту». Перезвонить в банк и проверить транзакции в официальном приложении.

Звонки с подменных номеров: Номера с чужими региональными кодами или от имени банка (например, 900). Защита: Не брать трубку, если код региона незнаком. Указать, что разговор записывается. Игнорировать звонки из WhatsApp/Telegram с номеров, связанных с банками.

Звонки из социальных сетей от госорганов: Мошенники представляются сотрудниками ведомств. Защита: Знать, что работникам госорганов запрещено звонить через мессенджеры.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Взлом аккаунта знакомого в соцсетях: Сообщения с просьбой о деньгах. Защита: Перезвонить знакомому, задать секретный вопрос. Настроить максимальную защиту личных кабинетов.

Поддельный аккаунт в Telegram: Копии аккаунтов знакомых. Защита: Проверить номер, привязанный к аккаунту, и историю чата (у подделок она пуста).

Сомнительный сайт: Фишинговые сайты, имитирующие легитимные ресурсы. Защита: Проверить адресную строку на опечатки, наличие HTTPS и сертификата, юридическую информацию магазина. Очищать историю браузера. Добавить к адресу сайта слово «жулики» для поиска отзывов.

Zerotrust (нулевое доверие): Принцип проверки любой информации. Защита: Всегда сомневаться в подлинности входящих сообщений и звонков.

Смартфоны: Уязвимости из-за слабых паролей или вредоносных приложений. Защита: Использовать двухфакторную аутентификацию (2FA). Завести отдельную банковскую карту для онлайн-платежей с минимальным балансом. Не скачивать APK-файлы из неофициальных источников.

Электронная почта: Вредоносные вложения или фишинговые письма. Защита: Открывать вложения только от доверенных отправителей. Проверять адрес отправителя на опечатки.

Онлайн-общение с «работодателем»: Выманивание данных под предлогом найма. Защита: Проверять легитимность компании, не предоставлять личные данные без подтверждения.

Фальшивые операторы сотовой связи: Попытки доступа к личному кабинету, например, на «Госуслугах». Защита: Проверять подлинность звонящего через официальные каналы.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Проголосуйте за мою дочь/сына: Мошеннические сайты для голосования. Защита: Игнорировать такие просьбы, проверять домен сайта.

Имитация пуш-уведомлений от банков: Поддельные уведомления о транзакциях. Защита: Проверять уведомления только в официальных банковских приложениях.

Звонок под видом умерших родственников: Эмоциональный шантаж. Защита: Перезвонить другим родственникам для проверки.

Схема «Мамонт»: Обман при оформлении покупок с маркетплейсов. Защита: Проверять продавцов и не переходить по подозрительным ссылкам.

Уведомления о посылках: Фишинговые ссылки в сообщениях. Защита: Не переходить по ссылкам от неизвестных отправителей.

Оплата штрафов через СПБ: Поддельные платежные формы. Защита: Внимательно проверять реквизиты платежа.

Практическая часть

Автором была проведена беседа с родственниками во время праздничного застолья, когда практически вся семья была в сборе. Тема кибермошенничества часто поднималась в разговорах, поэтому не менее восьми из двадцати описанных схем были известны участникам. Однако некоторые методы, такие как схема «Мамонт» (обман при доставке товаров с маркетплейсов), оказались новыми для большинства присутствующих.

В ходе обсуждения были разобраны реальные случаи, произошедшие с членами семьи:

Тетя получила SMS «от Сбербанка» с просьбой подтвердить перевод по ссылке. Она сразу распознала мошенничество и не перешла по ссылке.

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)
Сайт: akademnova.ru
e-mail: akademnova@mail.ru

Двоюродный брат чуть не стал жертвой фейкового сайта Avito с «суперскидкой» на iPhone. Он заметил ошибку в домене (av1to.ru) и закрыл страницу.

Бабушке звонил «внук», прося деньги на лечение, хотя единственная внучка (автор) была в соседней комнате.

В рамках беседы была проверена настройка двухфакторной аутентификации (2FA). У некоторых родственников она отсутствовала, но это было исправлено. Все участники установили автозапрет на оформление кредитов. Маленьким двоюродным братьям объяснили опасность скачивания APK-файлов с неизвестных источников, так как ранее они это делали. Были обсуждены все 20 схем мошенничества, разработаны семейные пароли и секретные вопросы для идентификации подлинных звонков. Мошенники постоянно совершенствуют методы, поэтому важно поддерживать «кибериммунитет» в тонусе — как свой, так и близких.

Выводы

Человек остается наиболее уязвимым звеном в системе кибербезопасности. Несмотря на технологическую сложность современных схем мошенничества, они по-прежнему эксплуатируют базовые психологические механизмы — страх, доверчивость, поспешность в принятии решений. При этом профилактические меры (критическая проверка входящей информации, использование технических средств защиты) оказываются значительно эффективнее попыток разрешения уже возникших проблемных ситуаций.

Особое значение имеет непрерывность образовательного процесса в области кибербезопасности, поскольку мошенники постоянно совершенствуют свои методы. Как показала практическая часть с семейным

Всероссийское СМИ
«Академия педагогических идей «НОВАЦИЯ»
Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.
(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru
e-mail: akademnova@mail.ru

обсуждением, даже разовое, но детальное информирование позволяет существенно повысить уровень защищенности. Технические средства (двухфакторная аутентификация, ограничения по кредитам, специализированные платежные карты) создают важный базовый уровень защиты, но должны подкрепляться осознанным поведением пользователей. Перспективы исследования включают разработку интерактивных образовательных платформ для повышения цифровой грамотности и анализ новых схем кибермошенничества.

Список использованной литературы:

1. Кравченко, А. А. Кибербезопасность: основы защиты в цифровой среде / А. А. Кравченко. — М.: Инфра-М, 2023. — 320 с.;
2. Schneier, B. Psychology of Security [Электронный ресурс] / B. Schneier. — URL: https://www.schneier.com/essays/archives/2008/02/the_psychology_of_se.html (дата обращения: 15.03.2025);
3. Федеральный закон РФ «О безопасности» от 28.12.2010 № 390-ФЗ (ред. от 14.04.2023) [Электронный ресурс]. — URL: http://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 20.02.2025).

Дата поступления в редакцию: 22.06.2025 г.
Опубликовано: 28.06.2025 г.