Имя: _____ **Дата:** _____ **Баллы:** _____

Онлайн-мошенничество и социальная инженерия Руководство по защите

Фишинг по электронной почте, поддельные домены, вишинг, мошенничество с техподдержкой, проверка по внешнему каналу, BEC

ОБЗОР ОБУЧЕНИЯ: ОНЛАЙН-МОШЕННИЧЕСТВО

ЗАЩИЩЁННЫЙ
ШИФРОВАНИЕ ДАННЫХ
Стандарт AES 256 бит

СООТВЕТСТВУЮЩИЙ
ГЛОБАЛЬНЫЕ СТАНДАРТЫ
Нормативные рамки GDPR и CCPA

НУЛЕВОЕ ДОВЕРИЕ
ПОЛИТИКА ДОСТУПА
Многофакторная аутентификация

Добро пожаловать! Этот пакет заданий проведёт вас через защиту от онлайн-мошенничества. Вы изучите поддельные фишинговые сайты, тактики социальной инженерии, мошенничество с техподдержкой, векторы мошенничества с банковскими переводами и методы проверки платежей.

КОНТРОЛЬНЫЕ ТОЧКИ РАБОЧЕГО ЛИСТА

- [ ] **Части 1-4: освойте кибербезопасность и предотвращение угроз.**
- [ ] **Части 5-7: решите кроссворд и головоломки «поиск слов».**
- [ ] **Части 8-9: решите кейсы и задание с шифром.**
- [ ] **Часть 10: изучите страницы часто задаваемых вопросов (базовый и продвинутый уровень).**
- [ ] **Часть 11: изучите 10 интересных фактов из реальной жизни.**
- [ ] **Дополнительно: задание «Думай быстро».**

Открыть руководство VPN.com по кибербезопасности

URL: https://www.vpn.com/ru/kiberbezopasnost/onlayn-moshennichestvo/

Ваша дорожная карта обучения: защита от онлайн-мошенничества

- Определите распространённые признаки мошенничества с поддержкой и доменов с опечатками (тайпосквоттинга).
- Внедрите протоколы проверки электронной почты (SPF, DKIM, DMARC) против подмены отправителя.
- Внедрите проверку транзакций по внешнему каналу, чтобы предотвратить мошенничество с деловыми банковскими переводами.

ИНСТРУКЦИИ К РУКОВОДСТВУ ПО ОНЛАЙН-МОШЕННИЧЕСТВУ

Ответьте на вопросы с выбором ответа и вопросы «верно/неверно», дополните предложения с пропусками, используя банк слов, сопоставьте определения и решите кроссворд и головоломку «поиск слов». Примените свои знания по теме: защите от онлайн-мошенничества. Завершите работу дополнительным заданием «Думай быстро».

ОНЛАЙН-МОШЕННИЧЕСТВО И ЗАЩИТА ОТ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ (ВВЕДЕНИЕ)

Онлайн-мошенничество использует особенности поведения людей: фишинг, всплывающие окна «поддержки», вишинг и мошенничество с банковскими переводами. Внеполосное подтверждение транзакций и правила домена SPF/DKIM/DMARC помогают блокировать векторы социальной инженерии на шлюзе.

ВНИМАТЕЛЬНО ПРОЧИТАЙТЕ КАЖДУЮ КОНТРОЛЬНУЮ ТОЧКУ И ВЫБЕРИТЕ ИЛИ НАПИШИТЕ ПРАВИЛЬНЫЙ ОТВЕТ.

Контрольная точка 1: Задание с выбором ответа

1 **1. Какой главный признак мошенничества с поддержкой?**

- A. Всплывающее окно, утверждающее, что ваша система заражена, и требующее позвонить по телефону
- B. Автоматическое обновление безопасности, загруженное из официального реестра
- C. Менеджер паролей отказывается подставлять учётные данные на корпоративном домене
- D. Фоновое резервное копирование файлов на внешний диск

2 **2. Какой приём использует поддельные домены отправителя, чтобы украсть банковские данные?**

- A. Фишинг по электронной почте
- B. Сканирование портов
- C. Внедрение в память
- D. Криптографическое уничтожение

3 **3. Что представляет собой мошенничество с банковскими переводами?**

- A. Обман жертв с помощью социальной инженерии, чтобы они отправили деньги на фальшивые корпоративные счета
- B. Шифрование системных баз данных с помощью полезной нагрузки программы-вымогателя
- C. Запросы к базам данных с помощью команд SQL-инъекции
- D. Резервное копирование системных файлов на автономные диски

4 **4. Зачем мошенники создают поддельные интернет-магазины?**

- A. Чтобы красть у покупателей данные кредитных карт и платёжные учётные данные
- B. Чтобы размещать таблицы базы данных для анализа вредоносного ПО в песочнице
- C. Чтобы ускорить доставку интернет-заказов
- D. Чтобы бесплатно тестировать новые дизайны сайтов

5 **5. Что означает вишинг?**

- A. Голосовое мошенничество по телефонным сетям с целью кражи учётных данных
- B. Сканирование локальных сетей на наличие незащищённых системных устройств
- C. Восстановление системных баз данных после несанкционированного взлома
- D. Запуск недоверенного кода в защищённых виртуальных контейнерах

Контрольная точка 2: Задание «верно или неверно»

6 Вопрос 6

6. Фишинговые мошенничества нацелены только на конечных пользователей, но никогда на руководителей («киты»).

○ Верно ○ Неверно

7 Вопрос 7

7. В поддельных доменах часто используются небольшие опечатки (например, amaz0n.com), чтобы имитировать надёжные бренды.

○ Верно ○ Неверно

8 Вопрос 8

8. Мошенничество с поддельной техподдержкой можно решить, предоставив звонящему удалённый доступ.

○ Верно ○ Неверно

9 Вопрос 9

9. Социальная инженерия использует психологию человека, например страх и срочность, чтобы обойти правила безопасности.

○ Верно ○ Неверно

10 Вопрос 10

10. Запросы на банковский перевод всегда следует проверять по независимым каналам связи.

○ Верно ○ Неверно

Контрольная точка 3: Вставьте ключевые термины

Прочитайте каждое предложение ниже и вставьте пропущенный термин из банка слов.

1. Мошеннические письма, обманывающие пользователей, называются _____ .
2. Веб-адреса, имитирующие доверенные бренды, — это _____ .
3. Голосовые мошенничества, нацеленные на банковские данные, называются _____ .
4. Всплывающее окно с требованием денег за удаление вируса — это ложная техподдержка, то есть _____ .
5. Чтобы подтвердить запрос на платёж, нужна внеполосная _____ .
6. Перенаправление деловых транзакций на счета воров — это _____ .

СЛОВАРНЫЙ БАНК СЛОВ

ВЕЙЛИНГ ВИШИНГ КРИПТОВАЛЮТА МОШЕННИЧЕСТВО ПОДДЕЛКИ
ПОДМЕНА ПРОВЕРКА ФИШИНГ

Напишите свои ответы здесь:

1.
2.
3.
4.
5.
6.

Контрольная точка 4: Сопоставление понятий о безопасности

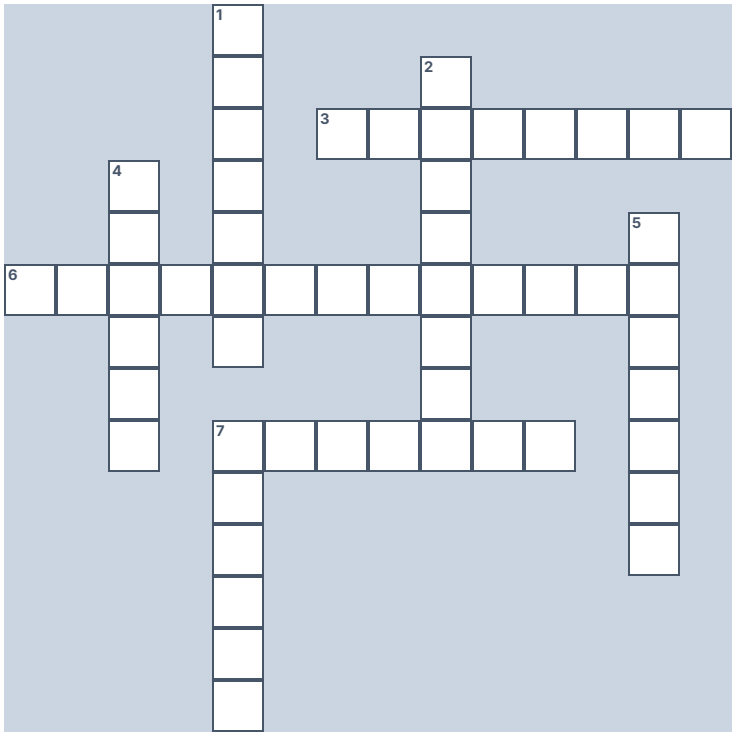
СОПОСТАВЛЕНИЕ ОПРЕДЕЛЕНИЙ

Сопоставьте каждый термин слева с правильным определением справа, введя соответствующую букву (A–H) в заполняемое поле.

☐	1. ФИШИНГ	A	Мошенническое перенаправление банковских транзакций на счета преступников.
☐	2. ПОДМЕНЁННЫЙ	B	Мошенническая схема, цель которой — украсть у жертв деньги или данные для доступа.
☐	3. ВИШИНГ	C	Отправка мошеннических SMS, чтобы похитить учётные данные мобильных аккаунтов.
☐	4. МОШЕННИЧЕСТВО	D	Мошеннические голосовые звонки, цель которых — украсть учётные данные и сведения об учётных записях.
☐	5. ПРОВЕРКА	E	Целевые фишинговые атаки, направленные на кражу учётных данных у топ-менеджеров уровня C.
☐	6. WIRE	F	Подделанный адрес отправителя письма или сайта, выглядящий как настоящий.
☐	7. ВЕЙЛИНГ	G	Мошеннические рассылки по электронной почте, цель которых — украсть учётные данные и пароли.
☐	8. СМИШИНГ	H	Подтверждение платёжных реквизитов через надёжный дополнительный способ связи.

Контрольная точка 5: Кроссворд

Решите кроссворд, вводя буквы в активные белые клетки. Номера соответствуют подсказкам ниже.



ПО ГОРИЗОНТАЛИ

3. Подтверждение платёжных реквизитов через надёжный дополнительный канал связи. (8)

6. Обманная схема, цель которой — украсть у жертв деньги или доступ к учётным данным. (13)

7. Целевые фишинговые атаки, нацеленные на кражу учётных данных у руководителей высшего звена. (7)

ПО ВЕРТИКАЛИ

1. Рассылка мошеннических SMS для кражи учётных данных мобильных аккаунтов. (7)

2. Имитация адреса отправителя письма или сайта, чтобы он выглядел легитимно. (8)

4. Мошеннические рассылки по электронной почте, цель которых — украсть логины и пароли. (6)

5. Мошенническое перенаправление банковских транзакций на счета преступников. (7)

7. Мошеннические голосовые звонки, цель которых — украсть учётные данные и данные счетов. (6)

Контрольная точка 5, альтернативный вариант: Доступные подсказки к кроссворду

Пользователи программ чтения с экрана и клавиатуры могут вводить ответы на кроссворд прямо в текстовые поля ниже.

ПО ГОРИЗОНТАЛИ

3 по горизонтали: Подтверждение платёжных реквизитов через надёжный дополнительный канал связи. (8 букв):

6 по горизонтали: Обманная схема, цель которой — украсть у жертв деньги или доступ к учётным данным. (13 букв):

7 по горизонтали: Целевые фишинговые атаки, нацеленные на кражу учётных данных у руководителей высшего звена. (7 букв):

ПО ВЕРТИКАЛИ

1 по вертикали: Рассылка мошеннических SMS для кражи учётных данных мобильных аккаунтов. (7 букв):

2 по вертикали: Имитация адреса отправителя письма или сайта, чтобы он выглядел легитимно. (8 букв):

4 по вертикали: Мошеннические рассылки по электронной почте, цель которых — украсть логины и пароли. (6 букв):

5 по вертикали: Мошенническое перенаправление банковских транзакций на счета преступников. (7 букв):

7 по вертикали: Мошеннические голосовые звонки, цель которых — украсть учётные данные и данные счетов. (6 букв):

Контрольная точка 6: Поиск скрытых слов

Найдите в сетке ниже 8 ключевых терминов. Слова могут идти по горизонтали, по вертикали или по диагонали.

С	М	И	Ш	И	Н	Г	П	А	Д	С	Д	Ж	И	К
Д	Х	Ф	П	Е	К	Ц	Р	Я	Ч	П	Ж	Ф	Ъ	Ж
А	Г	Н	И	Ш	И	В	О	А	Ф	О	Т	Р	У	Ш
Э	Н	Ф	М	Х	Ш	Ц	В	Г	Р	Д	Ю	В	З	Ц
И	И	Ь	Ы	Л	А	Х	Е	Я	Ю	М	Ю	Н	З	К
К	Л	П	Х	М	О	О	Р	Ч	Т	Е	И	У	Ф	И
Л	Й	Я	А	С	Ъ	З	К	Щ	В	Н	Ю	Ц	Ю	Б
Е	Е	И	О	Я	И	М	А	С	У	А	Р	Ь	В	О
Д	В	Я	Ю	З	Э	Т	Ы	Щ	Н	Щ	У	Б	С	Ъ
Д	Ш	О	И	Ъ	Г	Э	Щ	М	Х	Б	Ь	Я	Э	П
О	М	О	Ш	Е	Н	Н	И	Ч	Е	С	Т	В	О	Ц
П	Ф	Ь	К	Т	Д	А	Г	М	Ф	Ы	Ь	Ь	Н	Л
Й	Ш	Ф	И	Ш	И	Н	Г	Й	З	Б	Ж	К	Н	Ч
Ц	Ы	Х	Я	Е	Й	Ж	Ц	Г	А	О	У	В	Я	П
М	Ъ	Х	Щ	А	Ц	Ь	М	П	П	И	Й	Р	Й	Х

СПИСОК СЛОВ СЛОВАРЯ

ФИШИНГ ПОДДЕЛКИ ВИШИНГ МОШЕННИЧЕСТВО ПРОВЕРКА ПОДМЕНА ВЕЙЛИНГ СМИШИНГ

Контрольная точка 6, альтернативный вариант: Доступное сопоставление терминов

Сопоставьте каждый из 8 терминов из поиска слов с правильным определением, написав букву (A–H) на пустой строке.

ТЕРМИНЫ СЛОВАРЯ

- **A. ФИШИНГ**
- **B. ПОДДЕЛКИ**
- **C. ВИШИНГ**
- **D. МОШЕННИЧЕСТВО**
- **E. ПРОВЕРКА**
- **F. ПОДМЕНА**
- **G. ВЕЙЛИНГ**
- **H. СМИШИНГ**

ОПРЕДЕЛЕНИЯ И ПОЛЯ СОПОСТАВЛЕНИЯ

_____ 1. Имитация адреса отправителя письма или сайта, чтобы он выглядел легитимно.

_____ 2. Подтверждение платёжных реквизитов через надёжный дополнительный канал связи.

_____ 3. Мошенническое перенаправление банковских транзакций на счета преступников.

_____ 4. Рассылка мошеннических SMS для кражи учётных данных мобильных аккаунтов.

_____ 5. Целевые фишинговые атаки, нацеленные на кражу учётных данных у руководителей высшего звена.

_____ 6. Мошеннические голосовые звонки, цель которых — украсть учётные данные и данные счетов.

_____ 7. Мошеннические рассылки по электронной почте, цель которых — украсть логины и пароли.

_____ 8. Обманная схема, цель которой — украсть у жертв деньги или доступ к учётным данным.

Контрольная точка 7: Задание с перепутанными словами

Расставьте буквы ниже в правильном порядке, чтобы получить ключевые понятия и термины кибербезопасности. Запишите ответы в предусмотренные поля.

1. **ШФИНГИ** _____
2. **ГВШНИИ** _____
3. **ВРПЕРАКО** _____
4. **ГЕИЛНВЙ** _____
5. **ЕЛОИДПКД** _____
6. **НСИНТШВЕМ ОЧОЕ** _____
7. **ПНЕАОМД** _____
8. **МШГСНИИ** _____

Дополнительное задание: Думай быстро

ПО 3 ОТВЕТА В КАЖДОЙ КАТЕГОРИИ. ПОБЕЖДАЕТ ТОТ, КТО ПЕРВЫМ ЗАПОЛНИТ СПИСОК.

1	Устройства, которые могут быть взломаны			
2	Фразы, которые часто используют мошенники			
3	Способы оплаты, которые просят мошенники			
4	Виды онлайн-мошенничества			
5	Предложения, которые слишком хороши, чтобы быть правдой			
6	Места, куда можно сообщить о мошенничестве			
7	Слова, связанные с кибербезопасностью			
8	Люди, которых можно предупредить о мошенничестве			
9	То, для чего вы делаете резервные копии			
10	Тревожные признаки в электронном письме			
11	Признаки заражения компьютера			
12	Способы проверить интернет-магазин			
13	Способы защитить свои аккаунты			
14	Что делать, если вас обманули			
15	Что делать после утечки данных			

Контрольная точка 8: Кейсы по кибербезопасности

Примените изученные понятия к реальным ситуациям ниже.

КЕЙС 1: ПРЕДОТВРАЩЕНИЕ МОШЕННИЧЕСТВА С КОРПОРАТИВНЫМИ БАНКОВСКИМИ ПЕРЕВОДАМИ



Ситуация: Финансовый отдел получает срочное письмо с поддельного адреса поставщика с просьбой направлять будущие платежи по счетам на новый маршрутный номер.

Вопрос для обсуждения: Опишите политику проверки против мошенничества с банковскими переводами и укажите блоки аутентификации электронной почты.

КЕЙС 2: ФИШИНГОВЫЙ ИНЦИДЕНТ «КИТОБОЙ» С УЧАСТИЕМ РУКОВОДИТЕЛЯ



Ситуация: Руководитель перешёл по фишинговой ссылке, якобы ведущей к защищённому документу для заседания совета, и ввёл свои основные корпоративные учётные данные на поддельном портале.

Вопрос для обсуждения: Опишите шаги реагирования на инцидент и объясните, как провести аудит входов руководителей.

Контрольная точка 9: Расшифруйте шифр

Специалист по кибербезопасности защищает сетевые ресурсы от онлайн-злоумышленников. Используйте ключ «буква–число» ниже, чтобы расшифровать сообщение, вписав соответствующие буквы в пустые места.

КЛЮЧ ШИФРОВАНИЯ «БУКВА В ЧИСЛО»

А=1 Б=2 В=3 Г=4 Д=5 Е=6 Ё=7 Ж=8 З=9 И=10 Й=11
К=12 Л=13 М=14 Н=15 О=16 П=17 Р=18 С=19 Т=20 У=21 Ф=22
Х=23 Ц=24 Ч=25 Ш=26 Щ=27 Ъ=28 Ы=29 Ь=30 Э=31 Ю=32 Я=33

3	29	33	3	13	33	11	20	6		22	10	26	10	15	4

19	12	1	15	6	18	16	14		10		17	18	16	3	6	18	12	16	11

Расшифрованное сообщение:

СОВЕТ: КАЖДОЕ ЧИСЛО ОБОЗНАЧАЕТ ПОЗИЦИЮ ЭТОЙ БУКВЫ В АЛФАВИТЕ (НАПРИМЕР, 1 = А, 2 = Б, 33 = Я).

Контрольная точка 10: Базовые вопросы о кибербезопасности (Часть A)

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q1: Что такое онлайн-мошенничество?

Мошенническая схема, использующая цифровые каналы, чтобы заставить жертв отправить деньги или выдать личные учётные данные.

Q2: Каков главный признак фишингового письма?

Сообщение с требованием срочных действий (например, из-за блокировки аккаунта), направляющее вас по ссылке, не совпадающей с официальным доменом.

Q3: Что такое тайпосквоттинг?

Регистрация доменов с типичными опечатками популярных брендов (например, amaz0n.com) для размещения поддельных фишинговых сайтов.

Q4: Что такое мошенничество с поддельной техподдержкой?

Всплывающее окно, утверждающее, что ваш ПК заражён, и призывающее позвонить по номеру и заплатить за поддельную программу очистки или услуги удалённого доступа. [1]

Q5: Что такое вишинг?

Фишинговые атаки с использованием голосовых телефонных звонков, чтобы обманом получить данные банковского счёта или входа.

Контрольная точка 10: Базовые вопросы о кибербезопасности (Часть B)

Просмотрите частые вопросы и ответы о снижении онлайн-угроз.

Q6: Что означает мошенничество с использованием электронных средств связи (wire fraud)?

Перенаправление платёжных операций на мошеннические счета путём выдачи себя за поставщиков или руководителей.

Q7: Что такое вейлинг?

Высоконаправленная форма целевого фишинга, нацеленная прямо на ценные цели, такие как руководители высшего звена компаний.

Q8: Что такое смишинг?

Мошеннические текстовые сообщения, отправляемые на мобильные устройства, со ссылками на поддельные порталы или уведомления об отслеживании.

Q9: Почему так важна внеполосная проверка?

Подтверждает детали транзакции по отдельному каналу связи (например, телефонному звонку), избегая скомпрометированных цепочек писем.

Q10: Как работает мошенничество с поддельным эскроу-счётом?

Мошенники создают поддельный эскроу-сайт, утверждая, что средства надёжно удерживаются, а затем крадут банковский перевод покупателя.

Контрольная точка 10: Продвинутые вопросы о безопасности (Часть C)

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q1: Как мошенники используют BEC (компрометацию деловой переписки) для мошенничества с банковскими переводами?

Они взламывают учётную запись электронной почты настоящего сотрудника, следят за перепиской по счетам и присылают обновлённые платёжные реквизиты с мошенническими банковскими счетами.

Q2: В чём риск IDN-гомографических атак при онлайн-мошенничестве?

Использование символов, не входящих в ASCII и выглядящих как обычные буквы (например, кириллической «а»), для регистрации поддельных доменов, имитирующих настоящие бренды.

Q3: Почему проверка заголовков электронных писем важна при выявлении мошенничества?

Показывает реальный IP-адрес исходного сервера и статус проверки SPF/DKIM, выявляя, подделан ли домен отправителя.

Q4: Как мошенники, выдающие себя за техподдержку, используют программы удалённого доступа?

Они используют утилиты вроде AnyDesk или TeamViewer, чтобы подключиться к устройству жертвы, внедрить вредоносное ПО и украсть сохранённые пароли.

Q5: Какова цель мошенничества с авансовыми платежами?

Обман жертв, чтобы они заранее оплатили комиссию за обработку ради крупного денежного вознаграждения, которого не существует.

Контрольная точка 10: Продвинутые вопросы о безопасности (Часть D)

Изучите продвинутые технические аспекты систем безопасности, анализа вредоносного ПО и соответствия требованиям к данным.

Q6: Как мошенники используют профилирование в социальных сетях для целевого фишинга?

Они собирают сведения об организационной структуре компаний и именах сотрудников, чтобы составлять убедительные фишинговые письма для целевых атак.

Q7: Почему поддельные интернет-магазины предлагают огромные скидки?

Чтобы заманить покупателей на ввод данных кредитной карты и получить учётные данные для повторного использования или перепродажи на форумах кардеров.

Q8: Как записи DMARC блокируют фишинговые схемы?

DMARC позволяет владельцам доменов просить получателей помещать в карантин или отклонять почту, не прошедшую согласованные проверки SPF и DKIM, что блокирует прямую подделку отправителя. [5]

Q9: В чём угроза порталов для кражи учётных данных?

Поддельные страницы входа, неотличимые от Microsoft 365 или рабочих пространств Google, похищают учётные данные в момент их ввода.

Q10: Как службы безопасности сообщают о мошеннических доменах и отключают их?

Отправляя доказательства мошенничества на адрес для жалоб регистратора, хостинг-провайдеру и в реестр Google Safe Browsing.

Часть 11: 10 реальных фактов и выводов о кибербезопасности

Ознакомьтесь с реальными фактами об инцидентах безопасности, механизмах защиты и стандартах соответствия.

1. АНАЛИЗ БЕЗОПАСНОСТИ

Фишинг и подмена были самым часто регистрируемым видом преступлений в IC3 ФБР в 2025 году: 191,561 жалобы. [2]

2. АНАЛИЗ БЕЗОПАСНОСТИ

Компрометация деловой электронной почты (BEC) привела к потерям свыше 3 млрд долларов, о которых сообщили в IC3 ФБР в 2025 году. [2]

3. АНАЛИЗ БЕЗОПАСНОСТИ

Домены-двойники отличаются от настоящих названий брендов одним-двумя символами, поэтому при беглом взгляде их можно не заметить.

4. АНАЛИЗ БЕЗОПАСНОСТИ

Мошенничество с технической поддержкой в 2025 году привело к убыткам более 2,1 млрд $, о которых сообщено в IC3 ФБР. [2]

5. АНАЛИЗ БЕЗОПАСНОСТИ

Гомографические атаки выглядят одинаково в адресной строке браузера, если браузер не показывает punycode-конфигурации.

6. АНАЛИЗ БЕЗОПАСНОСТИ

SMS-мошенничество (смишинг) использует короткие срочные сообщения со ссылками, оставляя жертвам мало контекста для распознавания обмана.

7. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Атаки типа «вейлинг» нацелены на электронную почту руководителей, потому что они управляют доступом к крупным банковским переводам.

8. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Проверка изменений платёжных данных звонком по известному сохранённому номеру телефона — ключевая защита от мошенничества с переводами BEC.

9. БЕЗОПАСНОСТЬ: ВАЖНО ЗНАТЬ

Поддельные эскроу-сайты — распространённое мошенничество на онлайн-площадках: они выглядят как безопасный платёжный сервис, но крадут банковский перевод покупателя.

10. АНАЛИЗ БЕЗОПАСНОСТИ

Google Safe Browsing предупреждает пользователей, прежде чем они откроют сайты, помеченные им как фишинговые или содержащие вредоносное ПО.

Технические ссылки и источники

Учебное пособие и интерактивные головоломки составлены на основе мировых стандартов NIST, OWASP и требований к соблюдению правил конфиденциальности данных.

НАУЧНЫЕ И ОТРАСЛЕВЫЕ ИСТОЧНИКИ

[1] Federal Trade Commission. (n.d.). How To Spot, Avoid, and Report Tech Support Scams.

https://consumer.ftc.gov/articles/how-spot-avoid-and-report-tech-support-scams

[2] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] IETF. (2015). RFC 7489: Domain-based Message Authentication, Reporting, and Conformance (DMARC).

https://www.rfc-editor.org/rfc/rfc7489.html

Ответы: контрольная точка 1 – вопросы с выбором ответа

1 Вопрос 1

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой главный признак мошенничества с поддержкой? → Всплывающее окно, утверждающее, что ваша система заражена, и требующее позвонить по телефону

2 Вопрос 2

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Какой приём использует поддельные домены отправителя, чтобы украсть банковские данные? → Фишинг по электронной почте

3 Вопрос 3

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что представляет собой мошенничество с банковскими переводами? → Обман жертв с помощью социальной инженерии, чтобы они отправили деньги на фальшивые корпоративные счета

4 Вопрос 4

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Зачем мошенники создают поддельные интернет-магазины? → Чтобы красть у покупателей данные кредитных карт и платёжные учётные данные

5 Вопрос 5

Правильный ответ: A

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Что означает вишинг? → Голосовое мошенничество по телефонным сетям с целью кражи учётных данных

Ответы: контрольная точка 2 – верно или неверно

6 Вопрос 6

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: фишинг нацелен и на руководителей; вейлинг — это фишинг, направленный на высшее руководство.

7 Вопрос 7

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

В поддельных доменах часто используются небольшие опечатки (например, amaz0n.com), чтобы имитировать надёжные бренды.

8 Вопрос 8

Правильный ответ: Неверно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Неверно: если дать мошеннику, выдающему себя за поддержку, удалённый доступ, он сможет внедрить вредоносное ПО и украсть данные.

9 Вопрос 9

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Социальная инженерия использует психологию человека, например страх и срочность, чтобы обойти правила безопасности.

10 Вопрос 10

Правильный ответ: Верно

ПРИМЕЧАНИЕ ДЛЯ ПРЕПОДАВАТЕЛЯ

Запросы на банковский перевод всегда следует проверять по независимым каналам связи.

Ключи к словарю и критерии оценивания

Критерии оценивания для преподавателя: ставьте 1 балл за каждое верное сопоставление (всего 8 баллов) и за каждый контекстный термин (всего 6 баллов).

КОНТРОЛЬНАЯ ТОЧКА 4: ОТВЕТЫ – СОПОСТАВЛЕНИЕ ПОНЯТИЙ

G 1. ФИШИНГ	F 2. ПОДМЕНЁННЫЙ	D 3. ВИШИНГ	B 4. МОШЕННИЧЕСТВО
H 5. ПРОВЕРКА	A 6. WIRE	E 7. ВЕЙЛИНГ	C 8. СМИШИНГ

КОНТРОЛЬНАЯ ТОЧКА 3: ОТВЕТЫ – КЛЮЧЕВЫЕ ТЕРМИНЫ

1 ФИШИНГ	2 ПОДДЕЛКИ	3 ВИШИНГ	4 МОШЕННИЧЕСТВО
5 ПРОВЕРКА	6 ПОДМЕНА		

КОНТРОЛЬНАЯ ТОЧКА 6, АЛЬТЕРНАТИВНЫЙ ВАРИАНТ: ОТВЕТЫ – СОПОСТАВЛЕНИЕ СЛОВ

1 B – ПОДДЕЛКИ	2 E – ПРОВЕРКА	3 F – ПОДМЕНА	4 H – СМИШИНГ
5 G – ВЕЙЛИНГ	6 C – ВИШИНГ	7 A – ФИШИНГ	8 D – МОШЕННИЧЕСТВО

ЗАМЕТКИ ДЛЯ ПРЕПОДАВАТЕЛЕЙ К ОБСУЖДЕНИЮ

Ключевые термины:
Проверьте, могут ли учащиеся своими словами объяснить ФИШИНГ, ПОДМЕНЁННЫЙ и ВИШИНГ и привести пример для каждого термина.

Кейсы:
Попросите учащихся обосновывать свои рекомендации фактами из рабочего листа, а не мнениями.

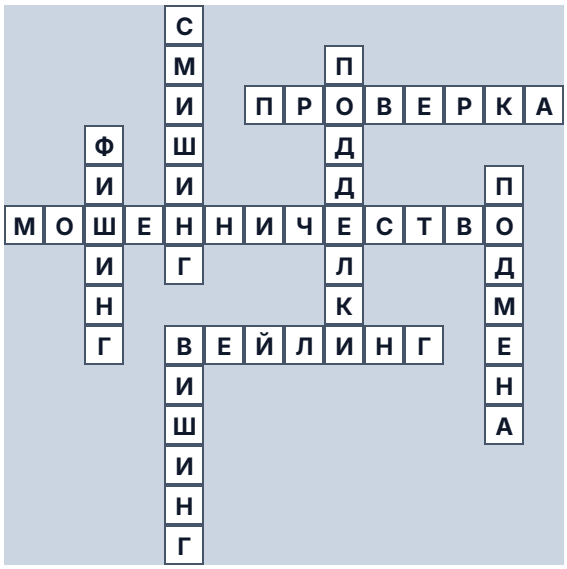
Оценка источников:
Попросите учащихся проверить хотя бы одно утверждение по источникам листа и обсудите, почему цифры, цены и правила со временем могут меняться.

Ключи к головоломкам и примечания для преподавателя

РЕШЕНИЕ К ПОИСКУ СЛОВ

С	М	И	Ш	И	Н	Г	П	А	Д	С	Д	Ж	И	К
Д	Х	Ф	П	Е	К	Ц	Р	Я	Ч	П	Ж	Ф	Ъ	Ж
А	Г	Н	И	Ш	И	В	О	А	Ф	О	Т	Р	У	Ш
Э	Н	Ф	М	Х	Ш	Ц	В	Г	Р	Д	Ю	В	З	Ц
И	И	Ь	Ы	Л	А	Х	Е	Я	Ю	М	Ю	Н	З	К
К	Л	П	Х	М	О	О	Р	Ч	Т	Е	И	У	Ф	И
Л	Й	Я	А	С	Ъ	З	К	Щ	В	Н	Ю	Ц	Ю	Б
Е	Е	И	О	Я	И	М	А	С	У	А	Р	Ь	В	О
Д	В	Я	Ю	З	Э	Т	Ы	Щ	Н	Щ	У	Б	С	Ъ
Д	Ш	О	И	Ъ	Г	Э	Щ	М	Х	Б	Ь	Я	Э	П
О	М	О	Ш	Е	Н	Н	И	Ч	Е	С	Т	В	О	Ц
П	Ф	Ь	К	Т	Д	А	Г	М	Ф	Ы	Ь	Ь	Н	Л
Й	Ш	Ф	И	Ш	И	Н	Г	Й	З	Б	Ж	К	Н	Ч
Ц	Ы	Х	Я	Е	Й	Ж	Ц	Г	А	О	У	В	Я	П
М	Ъ	Х	Щ	А	Ц	Ь	М	П	П	И	Й	Р	Й	Х

РЕШЕНИЕ КРОССВОРДА



РУКОВОДСТВО ДЛЯ ПРЕПОДАВАТЕЛЯ: РЕШЕНИЯ КРОССВОРДА

ПО ГОРИЗОНТАЛИ

3 по горизонтали: ПРОВЕРКА Подтверждение платёжных реквизитов через надёжный дополнительный канал связи. (8 букв)

6 по горизонтали: МОШЕННИЧЕСТВО Обманная схема, цель которой — украсть у жертв деньги или доступ к учётным данным. (13 букв)

7 по горизонтали: ВЕЙЛИНГ Целевые фишинговые атаки, нацеленные на кражу учётных данных у руководителей высшего звена. (7 букв)

ПО ВЕРТИКАЛИ

1 по вертикали: СМИШИНГ Рассылка мошеннических SMS для кражи учётных данных мобильных аккаунтов. (7 букв)

2 по вертикали: ПОДДЕЛКИ Имитация адреса отправителя письма или сайта, чтобы он выглядел легитимно. (8 букв)

4 по вертикали: ФИШИНГ Мошеннические рассылки по электронной почте, цель которых — украсть логины и пароли. (6 букв)

5 по вертикали: ПОДМЕНА Мошенническое перенаправление банковских транзакций на счета преступников. (7 букв)

7 по вертикали: ВИШИНГ Мошеннические голосовые звонки, цель которых — украсть учётные данные и данные счетов. (6 букв)

Ключ к словам-перевёртышам и шифру

Ключ для проверки заданий на расшифровку слов и «Секретного шифра».

КЛЮЧ К ЗАДАНИЮ «СОБЕРИ СЛОВО»

1.	ШФИНГИ	ФИШИНГ	5.	ЕЛОИДПКД	ПОДДЕЛКИ
2.	ГВШНИИ	ВИШИНГ	6.	НСИНТШВЕМОЧОЕ	МОШЕННИЧЕСТВО
3.	ВРПЕРАКО	ПРОВЕРКА	7.	ПНЕАОМД	ПОДМЕНА
4.	ГЕИЛНВЙ	ВЕЙЛИНГ	8.	МШГСНИИ	СМИШИНГ

КЛЮЧ К ЗАДАНИЮ С СЕКРЕТНЫМ ШИФРОМ

"ВЫЯВЛЯЙТЕ ФИШИНГ СКАНЕРОМ И ПРОВЕРКОЙ"

Ответы к кейсам

A Кейс 1: Предотвращение мошенничества с корпоративными банковскими переводами

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: финансовый отдел получает срочное письмо с поддельного адреса поставщика с просьбой направлять будущие переводы по счетам на новый маршрутный номер.
- Рекомендуемая стратегия и решение: Введите политику двойного подтверждения для всех платежей. Используйте внеполосную проверку по заранее сохранённому номеру телефона и блокируйте на шлюзе письма с поддельных доменов.

B Кейс 2: Фишинговый инцидент «китобой» с участием руководителя

Решение для преподавателя

РЕКОМЕНДАЦИИ ПО ОЦЕНИВАНИЮ

В ответах студентов должны быть отражены следующие пункты:

- Анализ ситуации: руководитель перешёл по фишинговой ссылке, якобы ведущей на защищённый документ для заседания совета директоров, и ввёл свои основные корпоративные учётные данные на поддельном портале.
- Рекомендуемая стратегия и решение: Изолируйте устройство руководителя. Сбросьте все корпоративные токены сеансов и учётные данные. Проверьте журналы доступа на предмет вывода данных и внедрите аппаратную MFA для всех входов.