

НЕЙРОНАУКА ФИШИНГА

GIULIANO PAIÃO

A man with dark, curly hair and a beard is shown in profile, looking towards a robot. The robot, which has a metallic, silver-colored head and torso with blue eyes, is holding a bright red apple in its right hand. The background is dark, making the subjects stand out.

КАК **ВЕРА, ЖАДНОСТЬ И УДОВОЛЬСТВИЕ**
ПРИВЕЛИ К ПОТЕРЯМ БОЛЕЕ
100 МИЛЛИАРДОВ ДОЛЛАРОВ

РЕАЛЬНЫЕ СЛУЧАИ АТАК
G20, НАТО, TWITTER (X) И МНОГОЕ ДРУГОЕ

АННОТАЦИЯ

Нейробиология фишинга

Как человеческие эмоции используются с хирургической точностью в кибератаках.

В этой книге Джулиано Пайао развенчивает ложное чувство безопасности, создаваемое брандмауэрами, надежными паролями и двухфакторной аутентификацией, и раскрывает наиболее уязвимую и часто используемую область цифровой безопасности: человеческий разум.

Книга «Нейробиология фишинга» исследует эмоциональные механизмы, которые делают кибератаки эффективными даже против опытных специалистов и компаний с развитой инфраструктурой. Вера, удовольствие и жадность — не просто эмоции, а когнитивные триггеры, которые при активации ослабляют критическое мышление и открывают путь к компрометации.

Используя доступный, но технически точный язык, автор представляет научные исследования, реальные примеры, методы социальной инженерии, инструменты с открытым исходным кодом, такие как GoPhish, и практические стратегии защиты от того, что не способен обнаружить ни один антивирус: человеческого поведения.

Это не просто книга о кибербезопасности. Это руководство по психологической войне, показывающее, что самые

масштабные атаки начинаются не со строк кода, а с образа мыслей.

Если вы работаете с людьми или данными либо принимаете решения, эта книга для вас.

ВСЕ ПРАВА ЗАЩИЩЕНЫ.

Данная книга защищена авторским правом. Никакая часть этой публикации не может быть воспроизведена, сохранена в информационно-поисковой системе или передана в любой форме и любыми средствами — электронными, механическими, посредством фотокопирования, записи или иным способом — без предварительного письменного разрешения автора, за исключением кратких цитат в академических, журналистских или критических целях.

Все имена, бренды, персонажи и ситуации, использованные в примерах из реальной жизни, были тщательно задокументированы и, при необходимости, адаптированы или анонимизированы для защиты личных данных.

Автор: Джулиано Пайао
© 2025 — Все права защищены.
1-е издание — Бразилия



Глава 1

Сердце — это новая конечная точка.

На протяжении десятилетий индустрия кибербезопасности развивалась, уделяя почти исключительное внимание технологиям: интеллектуальным межсетевым экранам, антивирусному программному обеспечению с передовыми эвристическими алгоритмами, многофакторной аутентификации и практически невзламываемому шифрованию. Но, несмотря на развитие технических средств, одна критически важная область оставалась уязвимой: **человеческий фактор**. И речь идёт не о любом аспекте человеческого поведения, а прежде всего об **эмоциях**.

Современные кибератаки уже не ограничиваются эксплуатацией уязвимостей операционных систем или приложений. Они нацелены на более глубокий и гораздо более уязвимый слой — **человеческий разум**. Социальная инженерия сделала большой шаг вперёд: это уже не просто психологический трюк. Сегодня она структурирована, изучена, автоматизирована и применяется с хирургической точностью. Её цель — не только устройства, но и ощущения, чувства, инстинкты.

«Люди, как правило, больше руководствуются своими глазами, чем руками; ибо каждый может видеть, но мало кто понимает, что видит».

Никколо Макиавелли

Сложный фишинг опирается не только на ссылки или технические уязвимости. В его основе лежат три универсальных психологических фактора, действующих независимо от культуры, социального положения и возраста: **вера, удовольствие и жадность**. Эти эмоциональные триггеры настолько сильны, что подавляют критическое мышление, приостанавливают логические рассуждения и делают любого человека уязвимым для компрометации. Каким бы неправдоподобным ни казалось сообщение, эмоциональная убеждённость способна подтолкнуть к клику. И ни одна система не может с уверенностью определить, действует ли пользователь под влиянием ложного обещания спасения, сиюминутного удовольствия или лёгкого богатства.

Именно в этот момент возникает настоящая уязвимость **нулевого дня современной** безопасности. Не та, о которой ещё не знают разработчики программного обеспечения, а та, что незаметно скрывается в человеческом подсознании. Это невидимая уязвимость, которую можно эксплуатировать, не оставляя журналов событий, не вызывая оповещений и не активируя антивирус. Уязвимость, которую каждый из нас носит в себе.

Важно понимать, что современные фишинговые кампании эволюционировали с точки зрения повествования, эстетики и методов. Злоумышленник уже не просто хочет, чтобы вы кликнули. **Он хочет, чтобы вы поверили. Он хочет вас. Он хочет того, что нужно вам.**

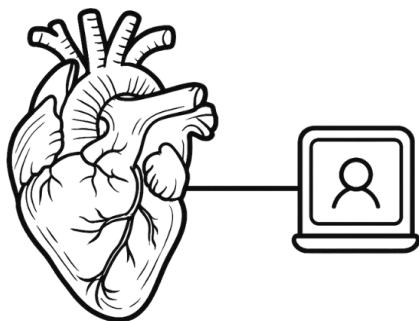
Анализ инцидентов последних лет выявляет закономерность: первоначальный доступ теперь всё чаще получают не с помощью сложных методов удалённой эксплуатации, а через, казалось бы, безобидные электронные письма и короткие, тщательно персонализированные сообщения, отправленные в нужный момент. Убедительная тема письма. Короткий текст, наполненный эмоциональным смыслом. Ссылка, поданная как нечто срочное. Один клик — и всё начинает рушиться.

В этой книге мы подробно рассмотрим эмоциональные механизмы, лежащие в основе самых изощрённых современных атак. Каждая глава будет посвящена одному из

трёх основных факторов — **ВЕРЕ, УДОВОЛЬСТВИЮ** и **ЖАДНОСТИ** — не как абстрактным понятиям, а как конкретным поверхностям атаки.

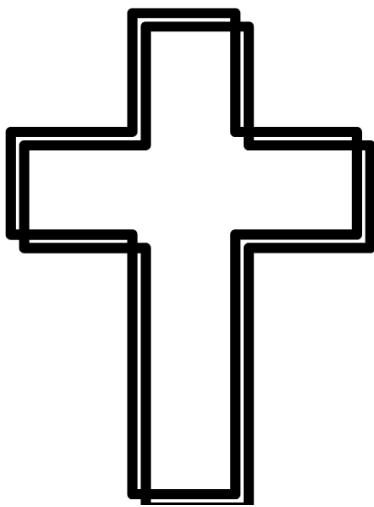
Мы представим научные исследования, реальные примеры и практические сценарии. Более того, мы покажем, как защищать организацию не только с помощью технологий, но и благодаря пониманию поведения и психологической зрелости.

Наибольшая уязвимость вашей компании может заключаться не в её системах, а в восприятии её сотрудников. Конечной точкой теперь является не только компьютер. **Новая конечная точка — сердце.**



Глава 2

РЕЛИГИЯ: ВЕРА КАК КОГНИТИВНЫЙ ИНСТРУМЕНТ



*«Религия использовалась основателями республик как
необходимый инструмент для поддержания
послушания и единства населения».*

«Рассуждения о первой декаде Тита Ливия»

Никколо Макиавелли

С самого зарождения цивилизации вера была одной из основ человеческого опыта. В палеолитических пещерах, храмах Древнего Египта, средневековых соборах и современных церквях стремление верить во что-то высшее неизменно сопровождало человечество. **Вера** дарит утешение, смысл и защиту от неопределённости. И именно потому, что она так глубоко укоренилась в человеке, его можно манипулировать.

Социальная инженерия, использующая религиозную тематику, — одна из наиболее эффективных форм психологического фишинга. В отличие от традиционных атак, эксплуатирующих технические уязвимости, этот подход направлен непосредственно на личные убеждения. Когда сообщение апеллирует к вере, оно обходит логические рассуждения и воздействует на эмоциональную сферу. Столкнувшись с тем, что кажется чудом, откровением или нападением на их убеждения, люди не анализируют сообщение внимательно — они реагируют.

В поляризованном мире, где дебаты о вере занимают место в парламентах, социальных сетях и на улицах, простая фраза

вроде «посмотрите, что они узнали о конце времен» может заставить тысячи людей мгновенно перейти по ссылке. И чем больше сообщение соответствует мировоззрению человека, тем эффективнее оно будет. Духовное любопытство превращается в цифровую импульсивность.

Фишинговые кампании с религиозным содержанием широко применялись в крупномасштабных атаках. Например, во время пандемии **COVID-19 по всему миру** распространялись электронные письма, авторы которых выдавали себя за духовных лидеров — пасторов, имамов и раввинов — и предлагали духовные наставления, просили о молитве или даже обещали чудесное исцеление. Многие из этих писем содержали ссылки на вредоносное ПО, которое после клика незаметно устанавливало бэкдоры на личные и корпоративные устройства.

Эту логику подтверждает исследование Раутледжа и Шарифа **«Религия и психология смысла»**, опубликованное в 2013 году: вера действует как эмоциональный и когнитивный стабилизатор. При её активации ослабевают механизмы сомнения и усиливается склонность к немедленным действиям. Эта особенность, столь ценная с человеческой точки зрения, превращается в уязвимость, когда ею манипулирует злоумышленник.

Практический пример

Мошенничество в церкви Святого Иоанна

Мотивация атаки

Вера и доверие обычно защищают и объединяют религиозные общины, но одновременно делают их привлекательными целями для фишинга. Мошенники знают, что верующие относятся к своим духовным лидерам с теплотой и уважением, поэтому религиозный авторитет легко превратить в инструмент эмоциональной манипуляции.

В мае 2023 года киберпреступники начали использовать именно эти узы доверия для совершения финансовых мошенничеств.

Кто был целью?

Целями стали прихожане **Епископальной церкви Святого Иоанна в США**, привыкшие получать сообщения от церкви по электронной почте. Простого появления нового имени — «мистер Лесли» — на официальном сайте прихода оказалось достаточно, чтобы злоумышленники запустили

мошенническую схему.

ИСПОЛЬЗОВАННАЯ ТЕХНИКА

1. Злоумышленники создавали поддельные электронные письма, выдавая себя за религиозных лидеров прихода, таких как мистер Лесли и отец Лонни.

2. Они использовали адреса электронной почты, похожие на официальные, но не принадлежавшие церкви.

3. Сообщения содержали эмоциональные и срочные призывы, например:

— «Мне срочно нужна помощь»;

— «Требуется немедленное внимание».

4. В письмах жертв просили купить подарочные карты и отправить их коды по электронной почте — распространённый способ перевода денег, который трудно отследить.

5. В некоторых случаях жертв перенаправляли на поддельные фишинговые сайты, чтобы похитить их финансовые данные.

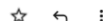
Разбор атаки

(no subject)  Inbox x



Rev. Lonnie Lacy <revlonnie.saintjohn@gmail.com>
to me ▾

12:41 PM (2 hours ago)



Hello Amanda, are you less busy at the moment? I have a request for you to manage confidentially. I will be into a meeting in few minutes, no calls so kindly respond via email.

Blessings!
Rev. Lonnie Lacy
Rector

From: "Rev. Lonnie Lacy" <lacylonnie.saintjohn@gmail.com>

Date: Thursday, October 6, 2022 at 2:34 PM

To

Subject: Re: Emily

Thanks for the swift reply, Here's what I want you to do for me because I think you are in the best position to do this for me discreetly.

I have been counseling and encouraging some cancer patients and aimed to reward them with " Gift Cards " this week to show how much we care about them.

This should be confidential until they all have the "Gift cards" as it's a surprise.

Can you get this done? and how soon? I will be responsible for the reimbursement personally.

ПОЧЕМУ АТАКА СРАБОТАЛА

Эксплуатация **ВЕРЫ** религиозными авторитетами создала ситуацию, в которой жертвы теряли бдительность. В конце концов, кто заподозрит просьбу, исходящую «от самого священника»?

Кроме того, использованный язык был простым и понятным и имитировал возвышенный тон церковных лидеров.

Психодинамика веры требует не доказательств, а принятия. Именно в момент такого безусловного принятия человек переходит по вредоносной ссылке, вводит учётные данные — и система начинает рушиться.

Для защиты от таких атак крайне важно не рассматривать пользователей исключительно как технический персонал. Обучение безопасности должно учитывать эмоциональный и социальный контекст. О религии следует говорить уважительно, но при этом ясно понимать, что религиозная тематика также может стать поверхностью атаки. Адаптивные фильтры, выявляющие новые шаблоны сообщений на религиозные темы, такие инструменты, как **VirusTotal**, **urlscan.io** и **MXToolbox**, а также анализ

кампаний по духовно-религиозным ключевым словам должны стать частью системы эмоциональной защиты.

Сегодня как никогда важно уважать веру и одновременно понимать её роль в современной киберсреде. В мире, где сообщения часто воспринимаются скорее эмоционально, чем рационально, настоящая защита начинается с понимания человеческой души.

Глава 3

Удовольствие: оргазм как триггер импульсивности

Человеческий разум устроен так, что стремится к вознаграждению. Среди естественных телесных вознаграждений сексуальное удовольствие занимает одно из самых высоких мест в иерархии желаний. Оно инстинктивно, иррационально и почти всегда трудно преодолимо. Этот импульс — не только биологическое переживание, но и уязвимость, которую весьма успешно эксплуатируют в кампаниях социальной инженерии.

В отличие от страха, который парализует, удовольствие мобилизует. Оно побуждает нас к действию, часто без раздумий. И именно эта модель автоматических действий делает удовольствие, особенно сексуальное, эффективным инструментом для разрушения систем и идентичностей.

В корпоративной среде стремление к приватности и сокрытию интимных подробностей создает идеальную почву для манипуляций. Никто не хочет признаваться в просмотре контента для взрослых в рабочее время. Никто не хочет, чтобы кто-либо знал о получении эротического

сообщения. Это молчание и стыд становятся союзниками злоумышленника.



*«Если бы человек контролировал свой язык и свои
сексуальные импульсы, многих войн удалось бы
избежать».*

Сократ

Спустя столетия мы по-прежнему уязвимы для тех же импульсов. В киберпространстве цена неспособности контролировать их особенно высока.

Один из самых известных случаев произошёл в 2020 году, когда фишинговая кампания распространялась через электронные письма, якобы отправленные коллегами. Тема письма была двусмысленной: **«Посмотри, что о тебе слили»**. В тексте содержалась ссылка на страницу, где якобы были размещены интимные фотографии жертвы или кого-то из её близких. Страница, копируя популярные сервисы обмена медиафайлами, требовала авторизации для просмотра фотографий. **Менее чем за 48 часов тысячи пользователей более чем из десяти стран передали злоумышленникам свои корпоративные учётные данные.**

Эти атаки эффективны, потому что воздействуют на лимбическую систему — область мозга, связанную с эмоциями и мотивацией. Согласно исследованию Pfaus et al. (2009) **«Нейробиология сексуального поведения»**, опубликованному в журнале **Frontiers in Neuroendocrinology**, оргазм активирует те же мозговые цепи вознаграждения, на которые воздействуют опиаты, такие как морфин. Это позволяет рассматривать сексуальное

удовольствие не просто как желание, а как мощный фактор, способный ослаблять рациональное суждение.

Пример из практики

КОГДА УЧАСТНИКИ G20 КЛИКНУЛИ НА ИНТИМНЫЕ ФОТОГРАФИИ

В воздухе витало напряжение. Это была встреча G20. Мировые лидеры собрались, секреты обсуждались за закрытыми дверями, решения, способные изменить курс мировой экономики, принимались в уединенных залах. И тут, среди дипломатии и протоколов, возникло желание.

На саммите, состоявшемся в Париже в 2011 году, делегаты и представители правительств Чехии, **Болгарии, Португалии, Венгрии и Латвии** начали получать ненавязчивые электронные письма с почти неотразимой темой:

«Посмотрите интимные фотографии Карлы Бруни».

Карла Бруни — бывшая первая леди Франции, известная модель, символ красоты и элегантности. Женщина,

неизменно привлекавшая внимание, в данном случае стала идеальной приманкой.

Ссылка казалась безобидной. В конце концов, кто заподозрил бы неладное посреди международной конференции, среди множества обязательств и конфиденциальной информации? Клик был быстрым, автоматическим, продиктованным любопытством. Именно на это и рассчитывали злоумышленники.

Разбор атаки



После перехода по ссылке устройства делегатов были незаметно скомпрометированы. **Троянская программа** установилась без видимых признаков и предоставила злоумышленникам полный удалённый доступ к компьютерам. Они могли наблюдать, прослушивать, перехватывать и отслеживать. Ничто больше не оставалось в безопасности. Желание взяло верх над здравым смыслом.

Согласно результатам расследования, источником атаки был **Китай**. Целью являлся шпионаж на высоком уровне. Стратегическая информация, секретные решения и внутренняя переписка оказались в распоряжении кибершпионов. То, что казалось всего лишь неловким электронным письмом, обернулось одним из крупнейших нарушений кибербезопасности на международном мероприятии.

Этот случай раскрыл тревожную тайну: независимо от уровня подготовки, опыта или важности цели, у всех нас есть эмоциональные слабости.

Там, среди министров и дипломатов, рухнула не только защита устройств, но и миф о неуязвимости, уверенность в собственной осмотрительности и, прежде всего, вера в то, что желание всегда можно обуздать разумом.

В этом и заключается истинная сила социальной инженерии: она разрушает не системы, а людей. Эта неврологическая реакция подразумевает, что, сталкиваясь с обещанием удовольствия, мозг снижает активность префронтальной коры — области, отвечающей за критическое мышление, оценку рисков и контроль импульсов. Именно поэтому даже опытные профессионалы, сталкиваясь с сексуальными соблазнами, совершают элементарные ошибки в обеспечении безопасности. В этом контексте «целчок» носит скорее эмоциональный, чем рациональный характер.

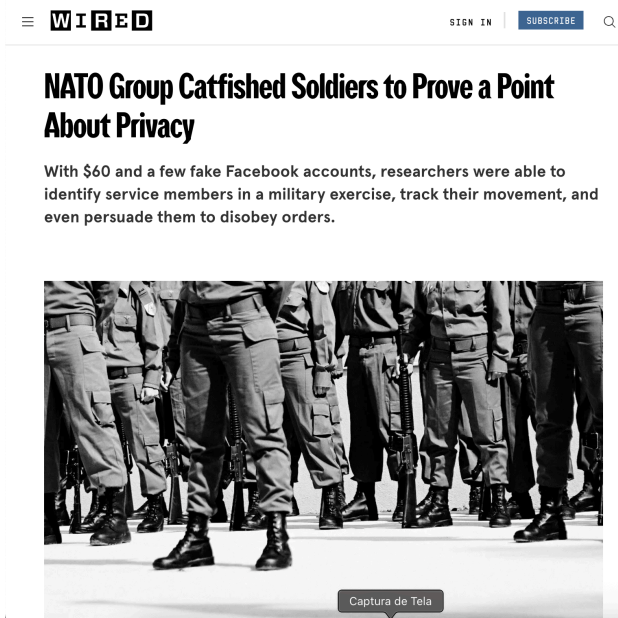
Пример из практики

Желание, которое поставило под угрозу солдат НАТО

Ещё одна известная кампания была направлена против военнослужащих. В 2018 году солдаты одной из военных баз **НАТО** получили в социальной сети запросы на добавление в друзья от якобы модели. Началась личная переписка: отправлялись двусмысленные фотографии и обещания интимных видео. Для их просмотра предлагалось **установить «новую версию» видеоприложения. На деле файл был троянской программой с функциями перехвата нажатий клавиш, утечки данных и скрытого закрепления в системе.**

Результат: многочисленные терминалы были скомпрометированы, а злоумышленники получили удалённый доступ к внутренним системам базы.

Разбор атаки



С точки зрения злоумышленника, сексуальный вектор прост в реализации и обеспечивает очень высокую отдачу. Для этого требуется лишь три элемента: вызывающее ассоциации изображение, правдоподобный сюжет и короткая ссылка. Жертва додумывает остальное, используя собственное воображение.

Для защиты крайне важно понимать, что подобную приманку нельзя считать табу. Игнорирование её существования не делает её менее эффективной. Компаниям необходимо включать тему удовольствия и сексуальности в программы повышения осведомленности. Внутренние кампании должны серьезно и уважительно, но твердо говорить о рисках эротической социальной инженерии.

С технической точки зрения возможны следующие меры по сдерживанию и предотвращению компрометации:

- I. **Мониторинг обращений к доменам с сомнительной репутацией, особенно связанным с порнографическим контентом.**
- II. **Блокировка сокращённых ссылок и внедрение систем предварительного просмотра URL-адресов.**
- III. **Использование интеллектуальных фильтров контента на основе машинного обучения, обученных выявлять шаблоны сексуализированного фишинга.**
- IV. **Имитация эротических фишинговых атак с использованием таких инструментов, как**

GoPhish, с отслеживанием метрик и целенаправленным обучением.

Кроме того, для проактивного обнаружения подобных кампаний можно использовать такие решения, как Cortex XSOAR, Proofpoint TAP и Zscaler, включая семантический анализ текста сообщений и встроенных изображений.

В конечном счёте удовольствие останется мощным мотиватором до тех пор, пока это желание остаётся плохо понятым. Задача современной безопасности — разрабатывать стратегии, защищающие людей от собственных импульсов. Ведь настоящая уязвимость заключается не во вредоносном коде, а в истории, которую жертва рассказывает себе, чтобы оправдать клик.

Глава 4

Жадность: ненасытное стремление к большему

Если удовольствие движет отдельным мгновением, то жадность — целыми проектами. Это более тихая эмоция, чем похоть, и менее спорная, чем вера, но не менее опасная. Жадность выглядит как законное стремление, цель, желание расти. Однако, когда ею манипулируют, она открывает лазейку, столь же серьёзную, как любая критическая уязвимость. Именно это и используют киберпреступники: человеческое стремление к большему — деньгам, престижу, удобству и прибыли.

В отличие от других эмоциональных триггеров, жадность социально приемлема и даже поощряется. Она присутствует в рекламных кампаниях, обещаниях чудодейственных курсов, финансовых гуру и преувеличенных меритократических рассуждениях. Именно поэтому трудно распознать в ней уязвимость системы безопасности. Но это так.

Социальная инженерия, движимая жадностью, стала одним из главных факторов, приводящих к цифровым компрометациям, особенно в корпоративной среде.

Руководители, стремящиеся к прибыли, сотрудники, ищущие дополнительного дохода, или даже обычные пользователи, ищущие быстрых возможностей, — все они являются потенциальными мишенями.

Яркий пример произошел в Бразилии в 2021 году во время бума инвестиций в криптовалюты. Распространялось электронное письмо с заголовком «Новая валюта обещает 300% роста за 15 дней — эксклюзивный анализ Forbes». В письме содержались поддельные графики и ссылки на клонированную инвестиционную платформу. При попытке регистрации жертвы вводили банковские реквизиты, личную информацию и даже отсканированные документы, удостоверяющие личность. Менее чем за три недели более 1200 человек стали жертвами мошенничества, а ущерб превысил 12 миллионов реалов.



«Людьми, как правило, движут две великие страсти: любовь и страх. Но мало кто способен устоять перед обещанием выгоды».

Никколо Макиавелли, «Государь»

Пример из практики

День, когда взломали Twitter

Обещание было простым, непреодолимым и разрушительным: **«Отправьте любую сумму в биткоинах и получите вдвое больше»**. Приманка была брошена, жадность стала крючком — и весь мир клюнул.

15 июля 2020 года Twitter, одна из крупнейших коммуникационных платформ мира, стала ареной одной из самых дерзких кибератак в современной истории. Верифицированные аккаунты — символы цифрового авторитета — превратились в инструменты мошенничества. **Илон Маск, Барак Обама, Apple, Uber** и многие другие стали марионетками в жестокой манипуляции. За кулисами стояли молодые люди с техническими знаниями и невидимым оружием — социальной инженерией.

Истоки атаки: когда на сцену выходит жадность

Всё началось с убедительной лжи. Но это была не просто ложь; это было обещание мгновенного богатства. Сообщение, завуалированное щедростью, рекламировалось через всемирно известные профили: «Мы помогаем

сообществу. Отправьте биткойны на этот адрес и получите вдвое больше за считанные минуты».

Жадность обращается непосредственно к самым примитивным механизмам человеческого разума. Стремление к лёгкой наживе подобно лесному пожару: оно быстро распространяется и выжигает логику. Менее чем за тридцать минут мошенники собрали более 100 000 долларов в биткойнах — лишь потому, что люди поверили, будто вот-вот удвоят свои деньги. Но никто не представлял, как именно хакеры проникли в нервную систему платформы.

Разбор атаки



En unos casos en el tweet se anunciaba que cualquier cantidad enviada llegaría doblada al usuario y en otras que las empresas hackeadas **donarían 10 millones de dólares** entre los seguidores.

Un hackeo que se salta la doble verificación

Esto, más allá de la estafa que entraña, también supone un grave problema de seguridad para una de las redes sociales más usadas en todo el mundo. Algunas cuentas hackeadas contaban con un **sistema de doble verificación** y aun así se ha podido penetrar en ellas.



ИНЖЕНЕРЫ-МАНИПУЛЯТОРЫ

Атака началась не со сложного кода, а с телефонных разговоров. Злоумышленники использовали старый, но эффективный метод — социальную инженерию. Выдавая себя за сотрудников ИТ-отдела Twitter, они связывались с реальными сотрудниками, завоёвывали их доверие и постепенно похищали учётные данные.

Такой подход называется целевым **фишингом (spear phishing)**: это персонализированная охота, в которой каждый шаг рассчитан на преодоление сопротивления и убеждение жертвы. Обманутые сотрудники предоставили злоумышленникам самое ценное — прямой доступ к административным инструментам компании.

КЛЮЧИ К КОРОЛЕВСТВУ

Получив доступ, хакеры скомпрометировали внутренний административный инструмент поддержки, который позволял сбрасывать пароли, изменять адреса электронной почты и получать полный контроль над учётными записями.

Представьте себе замок, ворота которого заперты на пароли и защищены системой аутентификации. А теперь представьте, что кто-то завладел главным ключом от всех этих ворот. Вот что и произошло. Злоумышленникам даже не понадобились настоящие пароли пользователей. С помощью внутреннего инструмента они смогли манипулировать всем, и сделали это с размахом.

ПОСЛЕДСТВИЯ

Было скомпрометировано около 130 учётных записей. Это были не обычные аккаунты, а символы авторитета, власти и глобального доверия: **Илон Маск, Джо Байден, Билл Гейтс, Apple и другие**. Казалось, все они распространяют одно и то же сообщение.

Атака проводилась точно. За считанные минуты тысячи людей по всему миру поверили, что участвуют в подлинной

благотворительной акции или получают знак благодарности. **Жадность** ослепила скептицизм: обещание финансовой отдачи от столь уважаемых имён казалось слишком убедительным, чтобы его подвергать сомнению.

КОНТРАМЕРЫ

Реакция Twitter была быстрой и вынужденной. Чтобы минимизировать ущерб, компания временно запретила верифицированным аккаунтам публиковать твиты. Впервые крупнейшие голоса платформы замолчали — из-за обнаруженной уязвимости.

Тем временем была сформирована рабочая группа для оценки масштабов провала. Начались внутренние расследования. Были привлечены агентства по кибербезопасности. Паника уже охватила всех, не только из-за украденных денег, но и из-за нарушения доверия.

В результате расследования были арестованы три человека. Лидером оказался семнадцатилетний подросток из Флориды — технически способный, но недостаточно зрелый и движимый тем же желанием, что и его жертвы: лёгкой наживой, признанием и властью.

Им были предъявлены обвинения в мошенничестве с использованием электронных средств связи, взломе системы и отмывании денег. Но этот случай показал нам нечто большее, чем просто уголовный процесс. Он продемонстрировал, насколько уязвимы для манипуляций со стороны человека даже самые мощные платформы.

Самая большая ошибка Twitter заключалась не в технической неполадке, а в человеческом факторе. Доверие, недостаток обучения, отсутствие многофакторной аутентификации для критически важных действий — всё это создало уязвимости, от которых не смог защитить даже самый лучший межсетевой экран.

Эта атака показала миру, что кибербезопасность — это не только технологии, но и психология. **Жадность нередко** становится самым слабым звеном цепи. Когда её эксплуатируют злоумышленники, она способна обрушить даже гигантов цифровой эпохи.

«Доверие строится по каплям, но теряется в ведрах».

Кевин Митник

Эта глава — не просто описание вторжения. Она отражает человеческую природу перед лицом обещания лёгких денег и служит предупреждением: пока существует **жадность**, **будут** существовать и те, кто готов ею воспользоваться.

Такие атаки работают не только благодаря привлекательной эстетике или дизайну сайта. Они воздействуют на внутренний нарратив: **«На этот раз всё получится»** или **«Кто не рискует, тот не выигрывает»**. Это модель эксплуатации, основанная на экономических надеждах.

Исследование Рао и Джорджа **«Жадность, зависть и принятие финансовых решений»**, опубликованное в 2016 году в **Journal of Behavioral and Experimental Economics**, показывает, что жадность активирует нейронные цепи, связанные со страхом и эйфорией. Она снижает самоконтроль, подрывает логическое мышление и заставляет игнорировать очевидные предупреждающие признаки. Обещание немедленной выгоды сводит благоразумие на нет.

В ходе симуляции, проведённой крупной американской консалтинговой компанией в сфере безопасности, команда red team разослала электронные письма 100 финансовым директорам публичных компаний. Тема была простой: **«Отчёт BlackRock со стратегиями увеличения капитала в ближайшие 30 дней»**. Семьдесят четыре человека

перешли по ссылке, пятьдесят два ввели данные на поддельной посадочной странице, а сорок шесть предоставили доступ к своей корпоративной электронной почте.

Эта статистика выявляет не просто техническую проблему, а поведенческий феномен — слепую жадность. Когда она проявляется на верхнем уровне иерархии, риск распространяется на всю организацию.

Для смягчения такого рода угроз крайне важно внедрять политику, выходящую за рамки традиционных информационных кампаний. Некоторые из таких стратегий включают в себя:

- I. Имитация фишинговых кампаний с использованием финансовых приманок: обещания бонусов, инвестиций, вознаграждений за производительность.**
- II. Поведенческий анализ, основанный на подозрительном взаимодействии с несанкционированными инвестиционными материалами.**

- III. Интеграция таких инструментов, как DNSTwist, Phishtank, OpenPhish и urlscan.io, для мониторинга клонов веб-сайтов брокерских фирм, инвестиционных платформ и банков.
- IV. Создание адаптивных фильтров на основе машинного обучения для обнаружения попыток мошенничества на основе лингвистического паттерна жадности.

С культурной точки зрения компаниям следует пересмотреть отношение к **«меритократии любой ценой»**. Корпоративная среда, поощряющая агрессивные и неэтичные системы вознаграждения, создаёт благодатную почву для иллюзии упущенной возможности.

Жадность, как и стремление к удовольствию, невозможно насытить. Каждое достижение открывает путь новым амбициям. Немецкий философ предупреждал:

«Мы живем в бесконечном цикле между желанием обладать и скукой после завоевания».

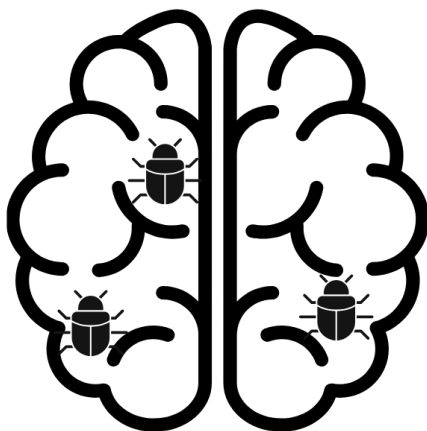
Артур Шопенгауэр

Именно этот механизм злоумышленники используют в качестве эмоциональной основы для манипуляций.

Ни одна компания не застрахована, и ни один человек не свободен от этого риска. Разница между безопасностью и компрометацией в данном случае заключается в способности распознать: то, что кажется слишком хорошим, чтобы быть правдой, почти всегда таковым и является. Когда инстинкт накопления перевешивает логику оценки, уязвимость уже эксплуатирована — ещё до клика.

Глава 5

«Нулевой день» человеческого разума



Термин **«нулевой день»** знаком любому специалисту по информационной безопасности. Он обозначает уязвимость, неизвестную разработчикам и поставщикам, для которой ещё нет исправления и которую можно незаметно эксплуатировать с разрушительными последствиями. На чёрном рынке особенно ценятся уязвимости нулевого дня, позволяющие удалённо выполнять код, повышать привилегии или сохранять незаметный постоянный доступ. Но существует разновидность таких уязвимостей, которую не найти в операционных системах, браузерах или фреймворках. Она скрывается в человеческом разуме.

В отличие от технических дефектов, когнитивную уязвимость нельзя исправить обновлением программного обеспечения. Это не ошибка в коде, а присущая человеку восприимчивость к манипуляциям. Такая невидимая уязвимость нулевого дня проявляется через когнитивные искажения, эмоциональные импульсы и модели поведения, сформировавшиеся в ходе эволюции. Её чрезвычайно легко эксплуатировать злоумышленникам, которые понимают человеческое поведение так же хорошо, как сети и протоколы.

К основным векторам эмоциональной эксплуатации относятся уже знакомые нам **ВЕРА, УДОВОЛЬСТВИЕ И ЖАДНОСТЬ**. Однако настоящая сила человеческой уязвимости нулевого дня проявляется в сочетании этих факторов с контекстом. Письмо с религиозным призывом может остаться незамеченным в обычный день, но оказаться чрезвычайно эффективным во время социальной нестабильности. Эротическая ссылка может быть проигнорирована в рабочее время, но стать неотразимой в период одиночества. Финансовое предложение может показаться подозрительным в стабильные времена, но правдоподобным в условиях экономического кризиса.

Эксплуатация эмоциональной уязвимости нулевого дня требует контекстного и персонализированного подхода. Современные злоумышленники используют разведку по открытым источникам (OSINT), чтобы глубоко изучить цель до отправки приманки. Они анализируют социальные сети, публичные комментарии, утёкшие списки адресов электронной почты, видимые предпочтения и модели взаимодействия, формируя психологический профиль. Такая практика, известная как эмоциональное профилирование, позволяет точно адаптировать фишинговое сообщение к убеждениям, желаниям и слабостям жертвы.

В ходе одного из тестов, проведённых компанией, специализирующейся на социальной инженерии, были созданы фишинговые письма на основе предварительного анализа профилей сотрудников. Команда использовала инструменты для изучения социальных сетей, форумов и других общедоступных данных. Один из сотрудников — отец троих детей и член местной религиозной группы — получил письмо с темой **«Срочная молитвенная кампания за больных детей — присоединяйтесь и поделитесь информацией»**. Ссылка вела на страницу, визуально идентичную официальному сайту организации, с формой «подтверждения участия». Введённые данные перехватывались злоумышленниками. Успешность кампании достигла 78 %, и тест был остановлен через семь минут после запуска.

Эта симуляция подтвердила то, что многие эксперты уже знают: самое слабое звено в безопасности — не техническое, а эмоциональное. А когда эмоции сочетаются со временем, контекстом и персонализацией, даже самый высококвалифицированный специалист не застрахован от этого.

Существует еще один отягчающий фактор. Образовательные и корпоративные системы учат

пользователей распознавать технические угрозы — расширения файлов, подозрительные URL-адреса, грамматические ошибки. Но мало кто знает, как распознавать эмоциональные угрозы. Никто не обучен распознавать, когда им манипулируют психологически. Эта неподготовленность превращает каждого сотрудника в скрытый вектор атаки.

Защита от уязвимостей человеческого разума начинается с признания собственной хрупкости. Осознание уязвимости — первый шаг к снижению риска. Организациям необходимо выходить за рамки традиционного обучения и инвестировать в эмоциональную грамотность, прикладную психологию безопасности и культуру критического мышления.

К числу практических действий относятся:

- i. **Формирование поведенческих профилей с использованием инструментов прогнозной аналитики;**
- ii. **Регулярные симуляции с контекстными и эмоционально насыщенными сценариями;**
- iii. **Обучение распознаванию манипуляций с акцентом на когнитивные искажения;**

iv. Привлечение психологов и специалистов по поведенческим наукам к программам повышения осведомлённости.

Человеческий разум — сложная система и, как любая система, подвержен сбоям. Отличие в том, что эти сбои невидимы для сканера, непредсказуемы для SIEM-системы и часто отрицаются самими жертвами. Именно поэтому человеческая уязвимость нулевого дня может быть самой опасной из всех.

*«Человеческая душа сильнее всего, кроме желаний,
которых она не понимает».*

Наполеон Бонапарт

Глава 6

Анатомия эмоционального взлома ОТ ПРИМАНКИ К КОМПРОМЕТАЦИИ

Эффективность атаки с применением социальной инженерии зависит не только от технического качества обмана, но и от того, как выстроен весь процесс. Подобно традиционной цифровой атаке, проходящей этапы разведки, эксплуатации, получения доступа и закрепления, эмоциональная атака также имеет логическую структуру. Различаются лишь используемые векторы: вместо сетевых пакетов и вредоносного кода применяются нарративы, психологические триггеры и тщательно подобранный язык.

В этой главе представлен полный разбор эмоциональной атаки: каждый этап рассматривается на основе реальных примеров и технико-поведенческой модели. Цель — показать, как человеческую манипуляцию можно систематизировать и воспроизводить с точностью, сопоставимой с разработкой вредоносной кампании.

РАЗВЕДКА

ЭМОЦИОНАЛЬНАЯ OSINT-РАЗВЕДКА

Любая атака начинается с информации. В случае эмоциональной социальной инженерии эта информация не ограничивается сетевой инфраструктурой или используемыми системами. Она фокусируется на поведении жертвы. Социальные сети, публичные комментарии, профили на профессиональных платформах, потребительские привычки и история взаимодействия предоставляют злоумышленнику обширную базу данных. С её помощью можно сделать выводы о религиозных убеждениях, сексуальных предпочтениях, финансовом положении, эмоциональных связях и даже моментах личной уязвимости, таких как горе или недавняя потеря работы.

В 2019 году атаку на сотрудницу отдела кадров международной компании подготовили на основе её публичной записи о смерти родственника. Через несколько дней она получила письмо якобы от службы психологической поддержки. Сообщение было составлено

деликатно и убедительно, а ссылка вела на поддельную страницу регистрации, требовавшую входа с корпоративным адресом электронной почты. Эмоциональная приманка точно соответствовала моменту её уязвимости.

На этом этапе широко применяются такие инструменты, как **Maltego**, **SpiderFoot** и **FOCA**, а также специализированные модули сбора данных на Python. Они позволяют сопоставлять общедоступные сведения, формировать досье и выявлять эмоциональные точки входа.

ПОДГОТОВКА НАРРАТИВА КОНСТРУКЦИЯ ПРИМАНКИ

Имея на руках эмоциональный профиль жертвы, злоумышленник начинает структурировать сообщение. Эта структура основана на принципах психологии убеждения. Для снижения критического мышления и стимулирования действий в контент применяются такие термины, как дефицит, срочность, авторитет, взаимность и социальное доказательство.

Язык играет ключевую роль. Электронные письма с намеренными опечатками встречаются всё реже. Сегодня

преступники инвестируют в профессиональный копирайтинг: короткие, лаконичные тексты, создающие максимальный эффект при минимальном сопротивлении. Цель — добиться быстрого эмоционального отклика, способного привести к автоматическому решению.

Пример: *«Вы были выбраны из числа самых верных членов нашей общины. Нажмите ниже, чтобы подтвердить свое участие в специальной встрече с духовными лидерами».* Содержание, изложенное в одном абзаце, затрагивает темы веры, статуса и страха упустить уникальную возможность.

РЕАЛИЗАЦИЯ

Первичный контакт и взаимодействие

После создания приманку распространяют по электронной почте, в личных сообщениях социальных сетей, через мессенджеры или даже по телефону. Цель — не просто клик, а эмоциональное вовлечение. Более сложные кампании предполагают первоначальный диалог, за которым следует призыв к действию. Такой подход распространён в романтическом мошенничестве, схемах с благотворительными пожертвованиями и финансовых манипуляциях.

Посадочная **страница** оформляется с той же тщательностью. Часто используются точные копии легитимных платформ. Такие фреймворки, как **SET (Social-Engineer Toolkit)**, **Evilginx2**, **BlackEye** и **Modlishka**, позволяют в реальном времени перехватывать файлы cookie, токены сессии и учётные данные, в том числе при наличии многофакторной аутентификации.

КОМПРОМЕТАЦИЯ

ПЕРЕДАЧА ДАННЫХ ИЛИ ВЫПОЛНЕНИЕ ДЕЙСТВИЯ

Компрометация может принимать разные формы: передача учётных данных, установка вредоносного ПО, банковский перевод, отправка документов или предоставление удалённого доступа. Во всех случаях успех зависит от глубины эмоциональной манипуляции. Чем сильнее вовлечена жертва, тем выше её доверие и готовность выполнить требуемое действие.

Успешные кампании социальной инженерии не просто собирают данные — они внедряют нарратив. Многие жертвы, даже поняв, что их обманули, с трудом признают ошибку, потому что история вызвала сильные эмоции. Это сопротивление мешает быстро реагировать на инцидент и способствует продолжению атаки.

ПОСЛЕ КОМПРОМЕТАЦИИ

Психологическое и техническое закрепление

После первоначальной компрометации злоумышленник может продолжать использовать эмоциональную связь. Например, в романтическом мошенничестве преступник поддерживает разговор, запрашивает дополнительные данные и прибегает к эмоциональному шантажу для расширения доступа. В корпоративной среде скомпрометированную почтовую учётную запись часто используют для отправки внутренних сообщений и атак на других сотрудников, эксплуатируя доверие между коллегами.

Закрепление происходит и на техническом уровне. Легковесные вредоносные программы, такие как инфостилеры и кейлоггеры, используют для сохранения доступа, наблюдения за действиями пользователя и подготовки новых, более сложных атак.

ВЫВОДЫ

Анализ эмоциональной атаки показывает, что мы имеем дело с чрезвычайно гибкой моделью эксплуатации. Она опирается не на уязвимости программного обеспечения, а на людей. Такая атака действует незаметно, с трудом отслеживается и часто не выглядит угрозой для традиционных средств защиты.

Распознавание каждого этапа этого процесса — первый шаг к противодействию. Защита должна выходить за рамки техники: необходимо развивать эмоциональный интеллект, критическое мышление, поведенческий анализ и, прежде всего, способность признавать, что **каждый человек — независимо от должности и происхождения — имеет уязвимость, которую можно эксплуатировать.**

Глава 7

РЕАЛИСТИЧНЫЕ СИМУЛЯЦИИ В GORPHISH: КАМПАНИИ НА ОСНОВЕ ЭМОЦИЙ

Теория необходима, но безопасность укрепляется только на практике. В этой главе вы шаг за шагом научитесь создавать реалистичную фишинговую кампанию на основе эмоциональных триггеров с помощью одного из наиболее эффективных инструментов с открытым исходным кодом — GoPhish. Он позволяет имитировать фишинговые атаки в контролируемой среде, собирать точные метрики и повышать устойчивость команды к реальным угрозам.

Внутренние симуляции предназначены не только для «проверки кликов». Они помогают понять, как, почему и когда люди кликают, и, что еще важнее, позволяют корректировать культуру, процессы и технологии.

Ниже вы найдете полное руководство, от установки до итогового отчета, посвященное кампаниям, основанным на эмоциональных триггерах, таких как вера, удовольствие и жадность.

ВВЕДЕНИЕ В GOPHISH

GoPhish — это бесплатная платформа для моделирования фишинговых атак с открытым исходным кодом, разработанная на языке Go. Она предлагает простой, интуитивно понятный и надежный веб-интерфейс для создания персонализированных кампаний, управления пользователями и просмотра результатов в режиме реального времени.

Требования:

- I. Операционная система: Windows, Linux или macOS
- II. Доступ в интернет для отправки электронных писем
- III. SMTP-учётная запись (реальная или тестовая — в зависимости от типа проверки)
- IV. Административный доступ (если потребуется открыть порты)

Загрузка:

- I. Посетите официальный сайт: <https://getgophish.com>
- II. Нажмите кнопку «Download Latest Release».
- III. Выберите соответствующую операционную систему.
- IV. Распакуйте файлы в папку по вашему выбору.

УСТАНОВКА И ВЫПОЛНЕНИЕ

В Windows:

- I. Распакуйте ZIP-архив.
- II. Откройте командную строку в папке с исполняемым файлом.
- III. Запустите gophish.exe.

В Linux/macOS:

- I. Распакуйте архив .tar.gz.
- II. Предоставьте файлу разрешение на выполнение:
- III. `chmod +x gophish`
- IV. Запустите: `./gophish`
- V. Административный интерфейс: `https://localhost:3333`
- VI. Сервер посадочных страниц: `http://localhost:80` (или другой адрес, указанный в конфигурации)
- VII. Имя пользователя по умолчанию: `admin`. Временный пароль генерируется при первом запуске и выводится в консоли или журнале GoPhish.

Рекомендуется сменить временный пароль сразу после первого входа.

НАЧАЛЬНАЯ КОНФИГУРАЦИЯ

SMTP (сервер отправки электронной почты)

Вы можете использовать:

- I. Внутренний корпоративный SMTP-сервер (идеально для внутренних тестов).
- II. Тестовый сервис, например Mailtrap (для контролируемой среды).
- III. Легитимный сервис, например Gmail или SendGrid (только при наличии разрешения).

ШАБЛОНЫ ЭЛЕКТРОННЫХ ПИСЕМ

Создавайте электронные письма, используя эмоциональный язык:

- I. Вера: «Срочное сообщение от вашей духовной группы»
- II. Удовольствие: «Доступно интимное видео — посмотрите прямо сейчас»
- III. Жадность: «Вы предварительно отобраны для получения бонуса в размере 3000 реалов»

ТЕХНИЧЕСКИЕ СОВЕТЫ

- I. Для персонализации используйте переменные, например {{.FirstName}}.
- II. Добавьте ссылки на подготовленные посадочные страницы.
- III. Включите отслеживание кликов и, при необходимости, сбор тестовых учётных данных — только в контролируемой и авторизованной среде.

СОЗДАНИЕ КАМПАНИИ ШАГ ЗА ШАГОМ

- I. Войдите в панель управления.
- II. Перейдите в раздел «Профили отправки».
- I. Настройте почтовый адрес отправителя и SMTP-сервер.
- II. Перейдите в раздел «Email Templates».
- III. Создайте или отредактируйте свой шаблон.
- IV. Вставьте тестовую ссылку с помощью переменной {{.URL}}.
- V. Перейдите в раздел «Landing Pages».
- VI. Создайте или импортируйте посадочную страницу и настройте сбор тестовых данных в соответствии с целями авторизованной проверки.
- VII. При необходимости включите сбор тестовых данных для отслеживания отправленных форм.
- VIII. Перейдите в раздел «Пользователи и группы».
- IX. Импортируйте пользователей (имя и адрес электронной почты).
- X. Данные можно импортировать в формате CSV.
- XI. Перейдите в раздел «Campaigns».
- XII. Придумайте название для кампании.
- XIII. Выберите группу пользователей.

- XIV. Выберите шаблон электронного письма.
- XV. Выберите профиль отправителя.
- XVI. Запустите кампанию.

ВЫПОЛНЕНИЕ И МОНИТОРИНГ

Как только кампания начнётся, вы увидите её в режиме реального времени:

- 1) Сколько писем было отправлено?
- 2) Сколько было открыто?
- 3) Сколько пользователей перешли по ссылке?
- 4) Сколько тестовых учётных данных было введено?

Для дальнейшего анализа вы можете экспортировать данные кампании в формате CSV или JSON.

ПРЕДСТАВЛЕНИЕ ИТОГОВОГО ОТЧЁТА

Для документирования и представления результатов моделирования следуйте следующей структуре:

Резюме для руководства

- ⇒ Цель моделирования
- ⇒ Тип использованной эмоциональной инженерии

Методология

- ⇒ Используемый инструмент (GoPhish)
- ⇒ Исследованные эмоциональные триггеры
- ⇒ Количество протестированных пользователей

Результаты

- ⇒ Показатель открытия электронных писем
- ⇒ Коэффициент кликабельности
- ⇒ Количество введённых тестовых учётных данных
- ⇒ Среднее время до реакции

Анализ

- ⇒ Какие триггеры оказались наиболее эффективными?
- ⇒ Существует ли корреляция с должностью, областью деятельности или профилем?

Рекомендации

- ⇒ Корректирующие действия
- ⇒ Необходимость специальной подготовки
- ⇒ Технические настройки защиты

Заключение

Симуляция эмоциональных атак — не просто техническая проверка, а поведенческая тренировка. Ответственно используя такие инструменты, как GoPhish, компания получает реальную защиту от современных угроз. Каждый клик — это урок, а каждый показатель — возможность для роста.

Глава 8

Контрольные списки эмоциональной и технической защиты

Защита от кибератак, основанных на социальной инженерии, требует большего, чем межсетевые экраны, антивирусы и политики паролей. Как показано в предыдущих главах, наиболее опасные векторы компрометации связаны не с техникой, а с человеческим фактором. Когда точкой входа становится эмоция — **вера, удовольствие или жадность**, — меры защиты должны сочетать эмоциональную грамотность, технические средства и стратегическое обучение.

В этой главе я представляю ряд контрольных списков, разделенных по контексту. Каждый из них может быть непосредственно использован на практике, будь то в профилактических мероприятиях, аудите или реагировании на инциденты.

Контрольный список мер эмоциональной защиты для сотрудников

Цель:

Цель — повысить осведомлённость сотрудников и их эмоциональную устойчивость к фишинговым кампаниям и психологическим манипуляциям.

- I. () Компания проводит ежемесячные или ежеквартальные тренинги по эмоциональной социальной инженерии.
- II. () Обучение включает в себя деликатные темы, такие как религия, сексуальный контент и финансовые обещания, с использованием соответствующего языка.
- III. () Сотрудники умеют распознавать фразы, вызывающие чувство срочности, дефицита и авторитета.
- IV. () Сотрудники могут сообщать о подозрительных сообщениях, не опасаясь наказания.
- V. () Существует понятный и доступный канал для сообщения о фишинговых письмах.
- VI. () Сотрудники подвергались симуляциям фишинга с персонализированными эмоциональными триггерами.

- VII. () Отдел кадров или руководство учитывают периоды повышенной эмоциональной уязвимости сотрудников (горе, увольнение, конфликт), которыми могут воспользоваться злоумышленники.
- VIII. () Существуют внутренние материалы или руководства по эмоциональной безопасности для индивидуального использования.
- IX. () Компания поддерживает культуру активного слушания, снижая изоляцию сотрудников и их восприимчивость к внешнему влиянию.
- X. () Периодически оценивается эмоциональное поведение сотрудников в связи с использованием цифровых коммуникаций.

Технический контрольный список для предотвращения атак, основанных на эмоциональном фишинге.

Цель:

Цель — обеспечить готовность инфраструктуры безопасности к выявлению, блокированию и обработке атак, основанных на социальной инженерии.

- I. () Активная фильтрация DNS блокирует вновь созданные домены или домены с низкой репутацией.
- II. () Реализована интеграция с такими источниками и инструментами, как **PhishTank**, **OpenPhish**, **VirusTotal API** и **urlscan.io**.
- III. () Похожие домены отслеживаются с помощью **dnstwist** для выявления тайпосквоттинга.
- IV. () Антивирус и EDR используют поведенческое обнаружение и интеграцию с данными об угрозах.
- V. () Анализ исходящего трафика для выявления подключений к подозрительным серверам после кликов.
- VI. () Механизм песочницы для предварительного анализа вложений и ссылок, полученных по электронной почте.

- VII. () В SIEM централизованно собираются журналы и настроены оповещения по словам и фразам, вызывающим эмоциональную реакцию (например: **«чудо», «срочно», «интимное видео», «быстрая прибыль»**).
- VIII. () Проверки SPF, DKIM и DMARC настроены корректно; письма, нарушающие политики аутентификации, блокируются или помещаются в карантин.
- IX. () Сегментация сети с ограничением бокового распространения после компромисса.
- X. () Многофакторная аутентификация (MFA) обязательна для электронной почты и внутренних систем, в том числе на мобильных устройствах.

Контрольный список по стратегическому менеджменту и организационной культуре

Цель:

Цель — согласовать эмоциональную и техническую безопасность с принципами лидерства, процессами и принятием организационных решений.

- I. () Руководители обучены выявлять методы социальной инженерии, направленные на высшее руководство.
- II. () Существует четкая политика обеспечения безопасной связи, в том числе в чрезвычайных ситуациях или при внутренней мобилизации.
- III. () Все руководители прошли симуляции фишинговых атак.
- IV. () Организация развивает сеть «амбассадоров безопасности» в подразделениях с высоким уровнем риска.
- V. () Действует политика оперативного реагирования на утечки или разглашение общедоступных данных команды.
- VI. () Информационные кампании обновляются на основе реальных событий (например, недавних нападений на компании в том же секторе).

- VII. () Организация инвестирует в языковое разнообразие в обучении (визуальное, текстовое, устное) для достижения различных когнитивных профилей.
- VIII. () Показатели эмоциональной зрелости и поведенческой устойчивости включаются в отчёты о рисках, связанных с человеческим фактором.
- IX. () В ежегодном плане повышения осведомленности предусмотрен бюджет, выделяемый на обеспечение эмоциональной безопасности.
- X. () Внутренняя коммуникация закрепляет безопасность как часть культуры, а не как систему наказаний.

Защита от эмоциональных атак — задача не только специалистов по безопасности. Она начинается с анализа индивидуального поведения, распространяется на организационную культуру и закрепляется техническими и образовательными процессами. Представленные контрольные списки служат практической основой для архитектуры защиты, которая не игнорирует человеческий фактор, а рассматривает его как центральное звено безопасности.

В следующем разделе собраны и пояснены ключевые термины социальной инженерии и эмоционального

фишинга, необходимые для единообразного понимания описанных методов и мер защиты.

Глава 9

Аннотированный глоссарий социальной инженерии и эмоционального фишинга

Для специалистов по информационной безопасности владение технической терминологией имеет первостепенное значение. Но в социальной инженерии и эмоциональной эксплуатации некоторые слова приобретают специфические и тонкие значения, превращаясь в инструменты, столь же мощные, как эксплойты и полезные нагрузки. Этот аннотированный глоссарий объединяет важнейшие термины книги, даёт ясные определения, контексты применения и практические пояснения.

1. Социальная инженерия

Определение: набор методов, использующих эмоциональные, психологические и поведенческие

особенности для манипулирования людьми с целью получения информации или доступа к системам.

Комментарий: человеческий эквивалент эксплуатации системных уязвимостей. Разница в том, что «полезной нагрузкой» здесь служит сам нарратив.

2. Фишинг

Определение: метод, использующий поддельные сообщения, обычно электронные письма, чтобы обманом заставить жертву раскрыть конфиденциальную информацию или совершить опасное действие.

Комментарий: в эмоциональном фишинге используются такие триггеры, как страх, вера, удовольствие или жадность, чтобы вызвать ощущение срочности, доверия или сопереживания.

3. Целевой фишинг (spear phishing)

Определение: персонализированный фишинг против конкретной цели, эффективность которого повышается при наличии её эмоционального профиля.

4. ВИШИНГ (ГОЛОСОВОЙ ФИШИНГ)

Определение: попытка мошенничества посредством телефонного звонка или голосового сообщения, при которой злоумышленник выдаёт себя за доверенное лицо или организацию.

Комментарий: часто применяется в схемах с поддельной технической поддержкой, кражей данных и эмоциональным вымогательством.

5. БЕЙТИНГ (ПРИМАНКА)

Определение: метод социальной инженерии, основанный на предложении чего-либо ценного — реального или мнимого — с целью заманить жертву.

Комментарий: примерами служат намеренно «забытые» USB-накопители или обещания эксклюзивного контента.

6. ПРЕТЕКСТИНГ

Определение: метод, при котором злоумышленник создаёт ложную историю, роль или личность, чтобы получить информацию либо побудить жертву к действию.

Комментарий: основополагающий принцип атак, основанных на авторитете или доверии. Например: «Я из ИТ-отдела, мне нужно сбросить ваши данные доступа».

7. ПСИХОЛОГИЧЕСКАЯ ПОЛЕЗНАЯ НАГРУЗКА

Определение: сообщение или эмоциональный элемент, созданный для немедленного воздействия и запуска автоматической реакции.

Комментарий: это не программное обеспечение, а фраза, изображение или заголовок. Например: «Ваше интимное видео попало в сеть».

8. ЭМОЦИОНАЛЬНЫЙ ТРИГГЕР

Определение: стимул, вызывающий определённую эмоцию, снижающий способность к рациональному анализу и повышающий импульсивность.

Комментарий: к основным эмоциям, рассматриваемым в книге, относятся страх, удовольствие, надежда, вина, жадность, вера и стыд.

9. ЧЕЛОВЕЧЕСКАЯ УЯЗВИМОСТЬ НУЛЕВОГО ДНЯ

Определение: эмоциональная или когнитивная особенность поведения человека или группы, которая ещё не была осознана и компенсирована средствами защиты.

Комментарий: пока компании ищут уязвимости с идентификаторами CVE в программном обеспечении, реальная точка входа может скрываться в неосознанных эмоциях.

10. OSINT (РАЗВЕДКА ПО ОТКРЫТЫМ ИСТОЧНИКАМ)

Определение: сбор и анализ общедоступной информации для изучения цели.

Комментарий: используется для создания подробных эмоциональных профилей на основе социальных сетей, блогов и публичных взаимодействий.

11. ПОВЫШЕНИЕ ОСВЕДОМЛЁННОСТИ

Определение: комплекс образовательных мероприятий, направленных на развитие знаний и навыков выявления угроз безопасности.

Комментарий: необходимо перейти от принципа «не переходите по ссылкам» к принципу «понимайте, как вами эмоционально манипулируют».

12. СИМУЛЯЦИЯ ФИШИНГОВОЙ КАМПАНИИ

Определение: контролируемый и авторизованный тест, имитирующий фишинговую атаку для измерения реакции пользователей.

Комментарий: если симуляция основана на эмоциональной инженерии, она превращается в полноценную программу поведенческого обучения.

13. ЦИФРОВАЯ ИМПУЛЬСНАЯ РЕАКЦИЯ

Определение: автоматическая и иррациональная реакция на онлайн-стимул.

Комментарий: цель эмоционального фишинга — спровоцировать именно такую реакцию.

14. ПСИХОЛОГИЧЕСКОЕ ЗАКРЕПЛЕНИЕ

Определение: психическое состояние, при котором жертва продолжает верить в предложенную версию событий даже после предупреждений.

Комментарий: подчёркивает важность эмпатии и психологической поддержки при реагировании на инциденты.

15. ЭМОЦИОНАЛЬНАЯ КУЛЬТУРА БЕЗОПАСНОСТИ

Определение: организационная среда, которая признаёт эмоции частью риска и инвестирует в поведенческую защиту.

Комментарий: компании, говорящие только о межсетевых экранах и многофакторной аутентификации, защищают не все точки входа.

Владение терминологией — один из инструментов защиты. Понимание не только определений, но и их практического применения помогает специалистам сочетать технический и человеческий подходы. Этот глоссарий призывает к постоянной эмоциональной бдительности.

Да благословит и защитит вас Бог.

Автор: GIULIANO PAIAO