Розв’яжи свою проблему з усмішкою

Я знайшов ідеальну пропозицію роботи. Здається, це вона знайшла мене

Як розпізнавати фальшиві вакансії та захищати особисті дані під час пошуку роботи



Max Paradox

Я знайшов ідеальну пропозицію роботи. Здається, це вона знайшла мене

Як розпізнавати фальшиві вакансії та захищати особисті дані під час пошуку роботи

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384906637

ALL-IN Rafał Płonkowski



ЗМІСТ

INTRO 5

Розділ 1 - Ідеальна пропозиція, або чому шахрай знає про твої кар’єрні мрії 11

Розділ 2 - Рекрутер нізвідки, або як працює позичена довіра 20

Розділ 3 - Найдорожчий безкоштовний рекрутинг, або коли кандидат починає платити 30

Розділ 4 - Анкета хоче знати все, або як не віддати особисте життя відділу HR 39

Розділ 5 - Подавай заявки всюди, нічого не перевіряй, або як втома від пошуку роботи допомагає шахраям 50

Розділ 6 - Співбесіда чи вистава? Як не втягнутися у фальшивий рекрутинговий процес 61

Розділ 7 - Усі вже заробляють, тільки ти ще вагаєшся. Пастка соціального доказу 73

Розділ 8 - Твоє резюме мандрує світом, або як зменшити непотрібні цифрові сліди під час пошуку роботи 83

Розділ 9 - П’ятнадцять хвилин, які можуть урятувати твої дані. Як перевірити вакансію перед поданням заявки 94

Розділ 10 - Безпечне подання заявки крок за кроком. Що надсилати, чого не надсилати й коли сказати «стоп» 104

Розділ 11 - У мене теж є запитання. Як розмовляти з рекрутером, щоб не стати легкою мішенню 114

Розділ 12 - Вітаємо, вас прийнято на роботу. Тепер перевір, що саме ти підписуєш.....124

Розділ 13 - Натиснув, надіслав, підтвердив. Що робити, коли підозрілий рекрутинг зайшов надто далеко.....134

Розділ 14 - Повідом про це, поки не зникли сліди. Як перетворити підозру в шахрайстві на конкретні дії.....145

Розділ 15 - Компанія існує, рекрутер існує, і шахрайство теж. Що робити, коли все виглядає справжнім.....157

Розділ 16 - Коли тобі справді потрібна робота. Безпека під тиском грошей і часу.....168

Розділ 17 - Мене ошукали. Як повернути спокій, довіру та сміливість продовжувати пошук роботи.....178

Розділ 18 - Безпечний пошук роботи без щоденного розслідування. Звички, які залишаються надовго.....188

Розділ 19 - Знову хтось мене знайшов. Як розпізнати загрозу, що повертається, перш ніж вона стане серйозною.....200

Розділ 20 - Ідеальна робота існує. Але їй не потрібен твій пароль. Як самостійно ухвалювати безпечні рішення..... 211

INTRO

Уяви собі: вівторок, 21:47. Ти саме переглядаєш чергове оголошення про роботу. Попередні дванадцять вимагали п’яти років досвіду, знання семи систем і вміння працювати в умовах стресу, що, найімовірніше, означає, що хтось кричатиме на тебе через месенджер. Тринадцяте оголошення виглядає інакше. Приваблива зарплата, гнучкий графік, дистанційна робота, швидке введення в курс справ і жодних абсурдних вимог. Компанія нібито динамічно розвивається, але цього разу не очікує, що ти розвиватимешся разом із нею безкоштовно.

Ти надсилаєш заявку. Через вісім хвилин приходить відповідь. Рекрутер у захваті від твого профілю, хоча за цей час він навряд чи встиг би навіть прочитати інструкцію до кавомашини. Він запрошує тебе до наступного етапу. Потрібно лише заповнити форму, надіслати фотографію документа, що посвідчує особу, і підтвердити банківські дані. Дрібна формальність. Зрештою, серйозна компанія повинна знати, з ким співпрацює.

І саме тут починається історія, яка може закінчитися не новою роботою, а дуже тривалим знайомством із гарячою лінією банку.

Фальшиві рекрутингові процеси - особливо неприємний різновид шахрайства, адже вони використовують цілком природне бажання людини знайти кращу роботу. Тобі зовсім не обов’язково бути наївним, необережним або надзвичайно вразливим до маніпуляцій. Достатньо втомитися від пошуків,

потребувати грошей або просто натрапити на пропозицію, яка настільки добре відповідає твоїм очікуванням, що на мить хочеться повірити в існування компанії, яка пропонує високу зарплату, повну свободу й керівника, який виходить на зв'язок лише тоді, коли йому справді є що сказати.

Шахраєві не потрібно переконувати тебе зробити те, чого ти не хочеш. Значно простіше пообіцяти саме те, що ти шукаєш.

Коли мрія отримує посилання на анкету

Ще не так давно підозріле оголошення іноді можна було впізнати за мовою. Хтось пропонував «великі грошики за маленька працювати», повідомлення виглядало так, ніби його переклав холодильник, а адреса відправника містила випадкові літери й назву компанії з трьома помилками. Сьогодні такі ознаки все ще можуть бути корисними, але їх уже недостатньо. Фальшиве оголошення може бути грамотно написаним, професійно оформленим і прикрашеним переконливим логотипом. Співрозмовник може використовувати галузеву термінологію, надсилати документи, схожі на справжні рекрутингові анкети, і навіть проводити співбесіду.

Останнє звучить особливо нахабно. Людина готує відповідь на запитання про свої найбільші слабкості, старанно пояснює перерву в трудовій діяльності, розповідає про професійний досвід, а по той бік екрана когось передусім цікавить, чи вдасться схилити її до розголошення конфіденційної інформації. Якби шахраї вкладали стільки зусиль у чесний бізнес, можливо, їм самим знадобився б відділ рекрутингу.

Проблема полягає в тому, що під час пошуку роботи обмін інформацією є цілком природним. У резюме містяться контактні дані, історія працевлаштування та відомості про освіту. Рекрутер може запитати, коли ти готовий розпочати роботу, на яку зарплату розраховуєш або який маєш досвід. Тому кандидат звикає відповідати на запитання й надсилати документи. Шахрай намагається скористатися цією звичкою, поступово зміщуючи межу між обґрунтованим проханням і вимогою, яка не має розумного зв'язку з поточним етапом відбору.

Не кожне прохання надати додаткову інформацію означає спробу шахрайства. Не кожна незвична розмова є обманом, так само як не кожне незграбно написане повідомлення надходить від злочинця. Справжні компанії також припускаються помилок, користуються послугами зовнішніх агентств і проводять рекрутингові процеси, логіка яких часом залишається загадкою навіть для самих рекрутерів. Тому ми не вчитимемося підозрювати всіх у всьому. Натомість навчимося відрізняти ситуації, які потребують звичайної уважності, від тих, коли необхідно зупинитися й перевірити, хто насправді нам пише.

Твої особисті дані - не вхідний квиток на співбесіду

Багато хто уявляє викрадення даних як видовищний злам комп'ютерної системи. Насправді ж іноді все починається з ввічливого повідомлення: «Для продовження процесу просимо заповнити додаткову інформацію». Залежно від сценарію шахрай може намагатися отримати фотографію посвідчення особи, дані для входу в обліковий запис, коди авторизації, фінансову інформацію або схилити кандидата до здійснення

грошового переказу. Він також може підсунути фальшивий сайт, підозрілий вкладений файл чи застосунок, нібито необхідний для проходження співбесіди.

Не всі ці дії спричиняють однакову шкоду. Сама лише адреса електронної пошти не надає комусь автоматичного доступу до твого банківського рахунку, а надсилання резюме не означає, що наступного ранку ти прокинешся з кредитом на купівлю яхти. Ризик залежить від виду розкритої інформації, обставин і подальших дій злочинця. Саме тому варто розуміти ці відмінності, а не впадати в паніку щоразу, коли надходить повідомлення з незнайомого номера.

Ми також поговоримо про тиск часу. Шахраї люблять ситуації, коли кандидат мусить ухвалити рішення негайно, тому що «пропозиція втрачає чинність», «залишилося лише одне місце» або «відділ HR закриває систему через п'ятнадцять хвилин». Цікава організація роботи: компанія нібито гарантує гнучкий графік, але її система найму поводиться як касир, що зачиняє магазин перед довгими святковими вихідними.

Поспіх сам по собі не доводить шахрайства, проте може заважати спокійно перевірити інформацію. А саме така перевірка часто потрібна нам найбільше.

Обережність не обов'язково означає параною

Ця книжка не має змусити тебе перестати відгукуватися на вакансії, видаляти кожне запрошення на співбесіду чи сприймати телефонний дзвінок від рекрутера як спробу захопити керування супутником. Мета полягає в тому, щоб знайти розумну рівновагу між

відкритістю до нових можливостей і захистом власних даних.

Ти дізнаєшся, як перевіряти вакансії, компанії, вебадреси та особи людей, які проводять відбір кандидатів. Побачиш, яку інформацію зазвичай можна надавати на різних етапах рекрутингу, коли варто поставити додаткове запитання, а коли краще припинити спілкування. Ми також розглянемо, що робити після натискання на підозріле посилання або надсилання особистих даних, адже усвідомлення загрози часто стає найважливішим саме тоді, коли щось пішло не за планом.

Ти не отримаєш чарівного списку слів, після появи яких кожна шахрайська схема негайно вмикатиме червону тривогу. Натомість отримаєш дещо практичніше: спосіб мислення, який допоможе оцінювати ситуацію навіть тоді, коли повідомлення виглядає переконливо, а співрозмовник звучить професійно.

Для початку запам’ятай одне запитання, до якого ми повертатимемося за різних обставин: чи можу я незалежно підтвердити, що ця людина справді представляє компанію, за яку себе видає? Не натиснувши на чергове посилання, надіслане тією самою людиною, а перевіривши інформацію через незалежний, надійний канал. Така невелика звичка здатна змінити перебіг усієї розмови.

Пошук роботи сам по собі буває виснажливим. Тобі зовсім не потрібна ще одна додаткова робота на посаді приватного детектива. Потрібні лише кілька добре підібраних правил, яких можна дотримуватися навіть після важкого дня, п’яти відхилених заявок і за майже повної відсутності бажання знову розповідати, ким ти бачиш себе через п’ять років.

Бажано - на роботі, яка справді існує.

І саме з цього ми почнемо.

Розділ 1 - Ідеальна пропозиція, або чому шахрай знає про твої кар'єрні мрії

Марта шукає роботу вже шість тижнів. Вона має досвід, актуальне резюме, добре оформлений професійний профіль і дедалі особистіші стосунки з автоматичними повідомленнями, що починаються словами «Дякуємо за зацікавленість». Вона відгукнулася на тридцять сім вакансій. Від семи компаній отримала відмову, дві запросили її на співбесіду, а решта, очевидно, перенесли процес найму в інший вимір, де час плине інакше й ніхто не перевіряє пошту.

Одного дня після обіду надходить повідомлення. Компанія шукає фахівчиню з обслуговування корпоративних клієнтів. Зарплата перевищує її очікування, робота дистанційна, графік гнучкий, а досвід Марти ідеально відповідає вимогам. Рекрутер пише ввічливо, конкретно й без дратівливого запитання про те, чи вміє вона працювати в умовах стресу. До того ж пропонує поспілкуватися ще сьогодні.

Марта відчуває полегшення. Нарешті хтось помітив її компетенції. Їй не доведеться вкотре доводити, що вона вміє користуватися електронними таблицями, спілкуватися з людьми й водночас не підпалювати офіс. Хтось прочитав її профіль і зробив правильні висновки.

Принаймні їй так здається.

Повідомлення могло надійти від справжнього рекрутера. Але воно також могло стати початком шахрайської схеми, у якій знання про професійний досвід

Марти є лише частиною ретельно підготовленої приманки. Найважливіше запитання поки що не в тому, чи чесна компанія. Воно звучить інакше: чому саме ця пропозиція так швидко завоювала її довіру?

Відповідь значно цікавіша за просте твердження, що людям подобається добре оплачувана робота.

Пропозиція, яка розуміє тебе краще, ніж попередній керівник

Фальшиві рекрутингові процеси часто використовують цілком звичайні потреби людей, які шукають роботу. Для однієї людини найважливішою буде стабільність, для іншої - можливість працювати з дому, а для третьої - швидкий заробіток, який дозволить сплатити найближчу орендну плату. Шахраєві не потрібно знати всю історію кандидата. Достатньо визначити потребу, навколо якої можна побудувати переконливу обіцянку.

Людина, втомлена від щоденних поїздок, зверне увагу на дистанційну роботу. Той, хто місяцями безуспішно подає заявки на початкові посади, зацікавиться оголошенням, яке не вимагає досвіду. Кандидат після втрати роботи може особливо гостро реагувати на інформацію про можливість негайно розпочати співпрацю. Усі ці реакції абсолютно природні. Проблема починається тоді, коли привабливість пропозиції підміняє оцінку її достовірності.

Варто помітити певний парадокс. Що краще оголошення відповідає нашим потребам, то сильніше ми прагнемо не помічати його слабких місць. Ми робимо це не свідомо. Розум просто починає шукати виправдання рішенню, яке емоційно ми вже ухвалили. Якщо пропозиція надзвичайно вигідна, можливо, компанія має

великий бюджет. Якщо відбір відбувається блискавично, напевно, їм терміново потрібен працівник. Якщо не вимагають досвіду, можливо, вони справді роблять ставку на потенціал.

Кожне з цих пояснень може бути правдивим. Проблема виникає тоді, коли всі вони народжуються виключно в нашій голові, а не випливають з інформації, яку можна перевірити.

Розгляньмо оголошення, що пропонує високу зарплату за кілька годин простих завдань на день. Не існує правила, за яким добре оплачувана робота обов'язково має бути складною або неприємною. Проте є цілком розумне запитання: за яку конкретно цінність компанія збирається платити? Якщо відповідь обмежується загальними фразами про виконання завдань, підтримку команди та роботу з платформою, кандидат не отримує достатньо інформації, щоб оцінити пропозицію.

У справжніх рекрутингових процесах також трапляються нечіткі описи посад. Різниця полягає в тому, що відбувається після запитання. Добросовісний представник компанії повинен мати змогу пояснити характер обов'язків або скерувати до людини, яка знає відповідь. Шахрай натомість може спробувати замінити пояснення черговою обіцянкою.

«Усе дізнаєтеся після реєстрації. Заробітки справді чудові».

Це відповідь, яка багато говорить про заробітки, якщо, звісно, вважати ентузіазм співрозмовника інформацією.

Три складові підозріло прекрасної пропозиції

Приваблива вакансія не стає фальшивою лише тому, що звучить вигідно. Однак варто перевірити, чи не

поєднує вона трьох характерних рис: надзвичайно сильної обіцянки, малої кількості конкретної інформації та очікування швидких дій.

Перша риса привертає увагу. Друга ускладнює оцінку реальної посади. Третя обмежує час, необхідний для виявлення проблем. Саме їхнє поєднання створює особливо небезпечну ситуацію.

Уяви оголошення: «Дистанційна робота, приваблива зарплата, повна гнучкість, початок негайно». Звучить приємно, але насправді незрозуміло, що саме тобі доведеться робити. Йдеться про обслуговування клієнтів, продажі, аналіз даних чи, можливо, сидіння перед комп'ютером із професійним виглядом дуже зайнятої людини? Коли ти запитуєш про обов'язки, тобі повідомляють, що подробиці стануть відомі після створення облікового запису на зазначеній платформі. Реєстрацію потрібно завершити протягом години.

На цьому етапі ще не потрібно виносити вирок. Достатньо помітити, що ти не отримав основної інформації, необхідної для ухвалення рішення, але від тебе вже очікують дій.

Тоді можна поставити три прості запитання:

- Які саме завдання я виконуватиму і на яких умовах?
- Яка компанія проводить відбір і де я можу незалежно підтвердити її участь?
- Чому зазначену формальність потрібно виконати ще до того, як мені нададуть основну інформацію?

Не йдеться про допит рекрутера з лампою, спрямованою йому в обличчя. Запитання можна поставити ввічливо, без звинувачень. Важливішим за тон є зміст відповіді. Конкретна інформація дозволяє

продовжити оцінювання. Ухиляння від відповіді, тиск або переведення розмови до чергових анкет дають підстави для підвищеної обережності.

Корисно також розділити два питання: чи приваблива для тебе посада і чи справді людина, яка з тобою зв'язалася, має право її пропонувати. Це незалежні питання. Навіть чудово описана посада не підтверджує особу рекрутера, а існування справжньої компанії не гарантує, що кожен, хто використовує її назву, є її представником.

Чому персоналізація працює

Повернімося до Марти. Її професійний профіль доступний публічно. Там є інформація про досвід обслуговування клієнтів, знання конкретних програм і зацікавленість у дистанційній роботі. Людина, яка готує фальшиве повідомлення, може використати ці дані, щоб створити враження індивідуальної зацікавленості.

«Ми звернули увагу на ваш досвід роботи з корпоративними клієнтами та знання CRM-систем».

Марта сприймає таке речення як доказ того, що рекрутер ознайомився з її компетенціями. Тим часом саме використання інформації з публічного профілю не підтверджує чесних намірів відправника. Персоналізація показує лише те, що хтось володіє певними даними.

Це важлива відмінність, адже сучасні інструменти дозволяють підготувати безліч повідомлень, які здаються індивідуальними, без реального аналізу кандидатів. Ретельно підібрані слова, грамотна мова й доречна згадка про професійний досвід підвищують довіру до контакту, але не є доказом його справжності.

Це не означає, що потрібно видаляти історію працевлаштування з інтернету. Професійний профіль існує, зокрема, для того, щоб тебе могли знайти справжні роботодавці. Однак варто знати, яка інформація є публічною та як її можуть використати. Якщо незнайома людина знає назву твого попереднього роботодавця, це не означає, що вона має спеціальні повноваження чи таємний доступ до кадрової документації. Можливо, вона просто прочитала профіль.

Комплімент також не є перевіркою. Фраза «Ви ідеальний кандидат» здатна покращити настрій, особливо після серії відмов, але сама по собі нічого не говорить про чесність відправника. Справжній рекрутер може щиро оцінити досвід кандидата. Шахрай може використати ті самі слова. Щоб розрізнити їх, потрібно перевірити щось більше, ніж компліменти.

Перший фільтр, який не позбавляє можливостей

Під час повсякденного пошуку роботи неможливо проводити багатогодинне розслідування щодо кожного оголошення. Якби кожна заявка вимагала роботи, порівнянної з аудитом міжнародної корпорації, кандидатові довелося б найняти асистента для пошуку працевлаштування. Тому варто почати з простого фільтра.

Перш ніж надсилати заявку, спробуй відповісти собі на чотири запитання: хто пропонує роботу, що саме потрібно робити, на яких загальних умовах і де можна перевірити існування цього набору. Якщо основна інформація доступна, пропозиція переходить до подальшої оцінки. Якщо її бракує, пошукай пояснення, перш ніж розкривати більш чутливі дані.

Припустімо, ти знаходиш вакансію адміністративного спеціаліста. Вказано назву компанії, перелік обов’язків, форму співпраці та спосіб зв’язку. Ти можеш самостійно знайти офіційний сайт роботодавця й перевірити розділ кар’єри. Відсутність оголошення на сайті ще не означає шахрайства, адже деякі компанії проводять набір через агентства або зовнішні портали. Проте ти можеш зв’язатися з компанією через незалежно знайдений канал і запитати про цей процес.

Така перевірка особливо цінна, коли хтось першим виходить із тобою на зв’язок, а ти не пам’ятаєш, щоб надсилав заявку. Чимало справжніх рекрутингових процесів починаються з повідомлення людині, яку знайшли в інтернеті. Отже, сам по собі несподіваний контакт не є сигналом тривоги. Але це вагома причина з’ясувати, хто саме тобі пише.

Якщо ти бачиш чудову пропозицію, але не можеш перевірити її походження, не обов’язково відразу її відхиляти. Можна тимчасово припинити передавання даних, попросити назвати компанію та перевірити інформацію поза каналом, запропонованим співрозмовником. Саме в цьому полягає різниця між обережністю та відмовою від будь-якої можливості.

Справжні гроші, фальшивий поспіх

Фінансовий тиск змінює спосіб оцінювання ризику. Коли ти маєш заощадження та стабільну роботу, пропозиція негайно розпочати співпрацю може здатися просто цікавою. Коли ж до кінця місяця тобі конче потрібен дохід, те саме повідомлення набуває зовсім іншого значення.

Немає сенсу вдавати, що достатньо просто зберігати холодну голову. Людина, яка хвилюється через рахунки, не стає автоматично спокійнішою після прочитання посібника з цифрової безпеки. Їй потрібен спосіб, який можна застосувати попри стрес.

Хорошим рішенням є відокремлення рішення зацікавитися пропозицією від рішення виконати конкретну дію. Ти можеш бути дуже зацікавлений у посаді й водночас відмовитися надсилати скан документа до підтвердження особи роботодавця. Можеш погодитися на співбесіду, але не встановлювати невідомий застосунок, що вимагає широких дозволів. Також можеш попросити час, щоб ознайомитися з умовами.

Така позиція не означає непрофесіоналізму. Добросовісний рекрутинговий процес вимагає співпраці обох сторін, а кандидат має право ставити запитання щодо процедури та захисту інформації. Якщо співрозмовник стверджує, що будь-яка спроба перевірки автоматично перекреслює твої шанси, ти отримуєш важливу інформацію про якість цього контакту.

Зрештою Марта не надсилає документ, що посвідчує особу, який у неї попросили ще до співбесіди. Натомість вона намагається підтвердити набір через офіційний контакт компанії. У нашій вигаданій історії з'ясовується, що підприємство не проводить такого відбору. Ми не знаємо, що сталося б далі, якби вона надіслала документ. Але знаємо, що вона зупинила процес саме в момент, коли ризик почав зростати.

Не кожна історія завершиться настільки однозначно. Іноді компанія підтвердить набір. Іншим разом отримати відповідь не вдасться, а пропозиція залишиться

неперевіреною. Тоді рішення доведеться ухвалювати за умов обмеженої інформації, пам'ятаючи, що можливість отримати роботу не виправдовує будь-якої вимоги.

Найважливіша зміна полягає в тому, щоб перестати сприймати привабливість пропозиції як аргумент на користь її справжності. Висока зарплата - це умова вакансії, а не доказ достовірності. Гнучкий графік - перевага, а не сертифікат безпеки. Ентузіазм рекрутера може бути щирим, але не замінює перевірки його особи.

Тож ти й надалі можеш радіти, побачивши вакансію своєї мрії. Можеш навіть на мить уявити перший переказ зарплати й новий підпис у корпоративній пошті. Проте перш ніж розкривати дані, зроби один зовсім неромантичний крок: перевір, чи за обіцянкою стоїть реальний роботодавець.

Ідеальна пропозиція роботи повинна витримати кілька розумних запитань. Якщо вона розсипається після першого, можливо, її найважливішою вимогою було саме те, щоб ти нічого не запитував.

Розділ 2 - Рекрутер нізвідки, або як працює позичена довіра

Телефон вібрує під час обіду. На екрані з'являється повідомлення від людини, яка представляється співробітником великої технологічної компанії. Відправник пише, що знайшов твій профіль на професійному порталі й хотів би запропонувати розмову про цікаву посаду. Підпис містить ім'я, прізвище, назву відділу та елегантну на вигляд вебадресу. Усе справляє враження професійного контакту.

Є лише одна дрібниця. Ти гадки не маєш, хто ця людина.

У цьому не було б нічого незвичайного, якби не той факт, що вже після двох повідомлень представник компанії пропонує перейти до приватного месенджера, а потім просить заповнити форму перевірки. Він пояснює, що це стандартна процедура безпеки. Важко відмовити процедурі безпеки, особливо коли хтось говорить про неї таким тоном, ніби її особисто затвердили п'ятеро юристів та одинадцять фахівців із захисту даних.

Тим часом справжнє запитання звучить так: звідки ти знаєш, що спілкуєшся саме з тією людиною, за яку себе видає відправник?

У першому розділі ми розглянули, як приваблива пропозиція завойовує увагу кандидата. Тепер займемося іншим механізмом. Шахрай може спробувати використати довіру, яку ти вже маєш до певної компанії, відомого рекрутингового порталу або професійного образу людини, яка веде розмову. Йому не потрібно

будувати власну репутацію. Достатньо переконливо позичити чужу.

Логотип - не документ, що посвідчує особу

Уяви два повідомлення. Перше надходить від невідомої людини, яка пропонує тобі взяти участь у якомусь незрозумілому проєкті. Друге містить назву відомої компанії, її логотип, підпис рекрутера та інформацію, що тебе обрали для попередньої співбесіди. Навіть якщо тексти обох повідомлень схожі, друге, найімовірніше, викличе більше зацікавлення.

Так відбувається тому, що впізнаваний бренд викликає певні асоціації. Компанія має історію, вебсайт, продукти, працівників і репутацію. Коли ти бачиш її назву, частина цієї довіри може автоматично переноситися на людину, яка нібито її представляє.

Це зручний механізм у повсякденному житті. Ми ж не перевіряємо з нуля надійність кожної установи, з якою контактуємо. Проблема полягає в тому, що в інтернеті назву компанії можна вписати в повідомлення без жодного дозволу. Логотип можна скопіювати, а службовий підпис підготувати за кілька хвилин. Сам зовнішній вигляд повідомлення не підтверджує його походження.

Шахрай може видавати себе за рекрутера відомої організації, представника агентства працевлаштування або співробітника платформи оголошень. Він також може створити вигадану компанію, яка завдяки професійному сайту та ретельно підготовленим матеріалам виглядатиме справжньою. В обох випадках мета однакова: переконати одержувача сприйняти заявлену особу як перевірений факт.

Це не означає, що кожне повідомлення з логотипом має викликати підозру. Фірмовий стиль - звичайний елемент професійного спілкування. Однак варто пам'ятати, що візуальна ідентифікація компанії та справжня особа відправника - це дві різні речі.

Якщо хтось представляється рекрутером відомого бренду, ти можеш перевірити, чи компанія справді набирає працівників на зазначену посаду. Також можна запитати через офіційний канал зв'язку, чи ця людина або агентство співпрацює з організацією. Важливо не будувати всю перевірку виключно на інформації, яку надає людина, чию особу ти намагаєшся встановити.

Це було б схоже на те, якби ти запитав підозрілого продавця, чи він точно не шахрай, а потім визнав його впевнене «Звісно, ні!» достатнім доказом. Ввічливість співрозмовника цінна, але вона не має сили офіційного посвідчення.

Адреса, яка здається знайомою

Одним із поширених елементів видавання себе за компанію є використання схожої вебадреси. Людина, яка готує фальшиве повідомлення, може використати домен, що нагадує справжню назву підприємства, або розмістити посилання на сайт, який імітує офіційний ресурс.

Деякі відмінності помітні відразу. Інші легко пропустити, особливо на телефоні, де довга адреса не вміщується на екрані. Додаткове слово, замінена літера або незвичне доменне розширення ще не доводять шахрайства, але потребують перевірки.

Наприклад, адреса, яка містить назву компанії, не обов'язково належить цій компанії. У домені rekrutacja-

przykladowafirma.example наявність слова «przykladowafirma» не доводить, що власником сторінки є справжній роботодавець. Так само посилання, яке починається з назви впізнаваного бренду, може вести на зовсім інший сайт, якщо справжній домен розташований в іншій частині адреси.

Тобі не потрібно ставати фахівцем із будови вебадрес, щоб зменшити ризик. Найпростіше правило таке: коли повідомлення вимагає виконати важливу дію, знайди офіційний сайт компанії самостійно, замість того щоб покладатися виключно на надіслане посилання. Можна скористатися раніше відомою адресою, власною закладкою або надійним джерелом. Потім перевір, чи є підтвердження рекрутингового процесу та зазначеного способу зв'язку.

Варто також знати, що символ замка біля адреси сайту не доводить чесності його власника. Насамперед він означає, що з'єднання зашифроване, а браузер може перевірити відповідні властивості з'єднання. Фальшивий сайт також може використовувати шифрування. Інакше кажучи, закритий замок не означає, що по той бік екрана сидить людина з відкритим серцем і бездоганною професійною біографією.

Ця деталь має практичне значення. Кандидат може побачити замок, професійний вигляд анкети та логотип роботодавця, а потім вирішити, що сайт безпечний. Тим часом жоден із цих елементів окремо не підтверджує, що документи потраплять до належного одержувача.

Справжній обліковий запис, несправжня роль

Видавання себе за рекрутера не завжди вимагає створення повністю вигаданої особистості. Шахрай може