Фішинг, вішинг, смішинг

і як з ними боротися

Якщо у вашій пошті немає спаму, це не означає, що вас не зламали.

Фішинг був і залишається одним з найпоширеніших векторів кібератак. За даними Acronis станом на першу половину 2022 року, майже 60% усіх зловмисних електронних листів, просканованих захисними продуктами компанії, були саме фішинговими. При цьому звичний «поштовий» фішинг є лише одним з різновидом цього багатоликого явища, яке використовує різні канали поширення і може бути як масованим, так і спрямованим на конкретну ціль.

Фахівці кажуть, що технології безсилі, якщо користувач легковірний. Використання штучного інтелекту і діпфейків робить шахрайські приманки ще більш переконливими. Проте є засоби і проти фішингу, які перевіряють і блокують підозрілі посилання. «МтБ» спробував розібратися в технологіях і різновидах цього небезпечного виду кібератак, а також у способах захисту від нього.

Розмаїття шахрайських прийомів

Фішинг — це атаки шляхом розсилки повідомлень та листів, що містять зловмисні вкладення або посилання, перехід за якими, своєю чергою, призводить до завантаження шкідливого ПЗ або відправляє жертву на підроблену веб-сторінку.

У звіті IBM Cost of a Data Breach 2023 зазначається, що фішинг є найпоширенішим вектором атак: торік на нього припадало 16% усіх випадків зламу мереж. Також фішинг на другому, після зловмисних інсайдерів, місці за критерієм заподіяної шкоди: в середньому $4,76 млн (компрометація ділової пошти — $4,67 млн). Від моменту фішингової атаки до її виявлення в середньому минає 217 днів, а на усунення наслідків потрібно ще 76 (для компрометації ділової пошти ці цифри відповідно 194 і 72, для соціальної інженерії 218 і 80).

Стратегій фішингу дві: масова і спрямована. У першому випадку розсилається велика кількість спам-листів у сподіванні на те, що хтось таки клюне. ***Spear phishing*** («полювання з острогою») — це атаки проти конкретних людей чи організацій. На відміну від звичайного фішингу, вони є персоналізованими. Для таких атак зловмисники збирають інформацію про жертву (її друзів та родичів, роботи, місця проживання, інших місць, де людина часто буває, нещодавніх покупок і т. ін.). Як влаштовані спрямовані фішингові атаки, показано на **рис. 1**.

Спрямовані атаки проти топ-посадовців компаній називаються ***Whaling*** («полювання на китів»). Зазвичай вейлінгові листи мають на меті спонукати жертву терміново перерахувати гроші на рахунок відправника. Навпаки, компрометація ділової пошти (***Business Email Compromise, BEC***) — це коли злочинці самі маскуються під топ-посадовця і від його імені дають розпорядження, наприклад, бухгалтерії.

Методик використання пошти для фішингу дуже багато. Найпростіший для

Рис. 1. Алгоритм спрямованої атаки типу spear phishing (джерело: TechTarget)

злочинців варіант — якщо вже є доступ до мережі організації, в цьому разі вони можуть відправляти листи з внутрішньої адреси. Якщо ж ні, використовуються техніки приховування або підміни посилань — наприклад, шляхом використання подібних символів, сервісів скорочення URL, оформлення вмісту у вигляді графічного зображення для обходу фільтрів тощо. Поява генеративного ШІ робить можливим створення реалістичних, граматично вивірених фішингових листів.

Окрім електронної пошти, існують інші канали поширення. ***Smishing*** — це розсилка SMS-повідомлень нібито від імені якоїсь компанії чи благодійної організації, де жертві пропонують зателефонувати, пройти за посиланням або відправити листа, після чого її просять ввести персональні дані. Оскільки на мобільних пристроях можуть використовуватись скорочені посилання, підробку може бути непросто одразу розпізнати. ***Vishing*** — це фішинг за допомогою телефонних дзвінків, часто за допомогою синтезованого голосового повідомлення про буцімто підозрілу активність банківського рахунку, в такий спосіб злочинці намагаються видурити у жертви інформацію про обліковий запис, номери банківських карток тощо.

Ще один вид фішингу називається, трохи неоковирно, ***Angler phishing*** («риболовля на вудочку»). Це полювання у соцмережах. Хакер створює фейкову сторінку, вдаючи службу підтримки якоїсь компанії, і контактує з клієнтами чи покупцями цієї компанії, які скаржилися на неї в соцмережі. Хакер намагається переконати їх повідомити персональні дані або перейти за посиланням, що призведе до завантаження шкідливого ПЗ. Такі атаки можуть бути доволі успішними, тому що зазвичай від скарги в соцмережах до реакції може пройти кілька годин, або вона взагалі залишається без відповіді. Тому користувачі раді отримати відповідь і, так би мовити, легко «ловляться на вудочку».

Дослідження Proofpoint

Статистику фішингу оприлюднила компанія Proofpoint у своєму звіті State of the Phish 2023, опитавши 7,5 тис. працівників і фахівців з IT-безпеки з 15 країн. Proofpoint констатує, що порівняно з попереднім (2021-м) роком обізнаність людей про фішинг дещо збільшилась (на 2–3%). Як показало опитування, 89% учасників знають, що треба стерегтися неочікуваних листів; 84% — що вкладення можуть містити небезпечне ПЗ. Також покращується розуміння більш тонких аспектів фішингу; зокрема 42% знають, що кіберзлочинці можуть надсилати по кілька листів, щоб завоювати довіру. Водночас 21% користувачів не знають, що відправник листа може видавати себе за іншого; 44% — що знайомий бренд ще не означає, що поштова адреса безпечна; 63% — що адреса в листі може не відповідати вебсторінці, куди вона веде.

Ситуацію ускладнює сформована після COVID-19 «нова нормальність», яка розмила межу між робочим і домашнім просторами. 78% респондентів зізналися, що використовують робочі пристрої у приватних цілях, 72% використовують особисті пристрої для

роботи, і 48% дозволяють родичам і друзям користуватися своїми робочими пристроями, хоча цей показник порівняно з 2021-м роком впав на 10 п.п. — ймовірно, тому, що люди стали знову більше часу проводити в офісах.

З-поміж респондентів Proofpoint 84% повідомили, що у 2022 році вони чи їхні організації зазнали принаймні однієї успішної фішингової атаки з використанням електронної пошти, 54% — що таких атак було три або й більше. За підрахунками компанії, найпоширенішим є, власне, масовий фішинг (з ним стикалися 85% респондентів). Загалом частота різних атак є сталою з року в рік і залишається на високому рівні. Зокрема атаки типу spear phishing зафіксували 74% респондентів, BEC — 75%, smishing — 75%, vishing — 71%, через соцмережі — 74%.

Що стосується наслідків фішингу, то 30% організацій, які стали жертвами успішних атак, зазнали безпосередніх фінансових збитків через фальшиві рахунки, обманні перекази коштів або зміну рахунків для зарахування заробітної плати (payroll redirection). Найпоширенішими наслідками є витік даних (44%), зараження здирницькими програмами (43%) і компрометація облікових записів (36%), усі три можуть бути легко монетизовані кіберзлочинцями.

У 2022 році Proofpoint зафіксував майже 1,6 тис. фішингових кампаній, які включали зловживання брендами. У цих випадках зловмисники користуються довірою користувачів до відомих фірм, використовуючи у повідомленнях їхній логотип або візуальний стиль. Найчастіше підробляють Microsoft: впродовж 2022 року було зафіксовано понад 30 млн повідомлень, в яких використовувалась символіка цього виробника або згадувались його продукти, такі як Office або OneDrive.

Proofpoint констатує, що хоча багатофакторна автентифікація (MFA) залишається одним з найкращих методів захисту, кіберзлочинці вже мають різні методи для її обходу. Такі атаки є технологічно складними, але деякі постачальники послуг Phishing-as-a-Service вже включають обхід MFA у свої фішингові пакети.

Зведення AAG IT Services

Ця британська консалтингова компанія також називає фішинг найпоширенішим видом кібератак. Зокрема, у 2021 році на фішинг припадало 43% атак в країнах Азії, 47% в Північній і Латинській Америці, тоді як у Європі він на другому місці (42%) після експлуатації вразливостей (46%). Загалом у світі 60% кібератак, спрямованих проти енергетичного сектору, мали фішингову складову; фінансового — 46%, виробничого — 40%, ритейлу — 38%.

У 2021 році жертвами фішингових атак у світі стали майже 324 тис. користувачів Інтернету, тобто загалом половина усіх жертв кібератак, і це попри твердження Google, що його засоби захисту блокують 99,9% фішингових спроб. Середні збитки від фішингу складають $136, а загалом у 2021 році хакери розжилися на $44,2 млн. Spear phishing використовують 65% хакерських угруповань, переважно з метою збирання інформації.

Згідно статистики від 2021 року, середній відсоток відкриття фішингових листів був на рівні 17,8%. Більш націлені кампанії, які включали телефонні дзвінки, були утричі ефективнішими — 53,2%. Цікаво, що мілленіали і зумери (групи віком 18–40 років) частіше ловляться на фішингові атаки (23%) порівняно з представникам покоління X (41–55 років), де цей показник складає 19%.

Повідомляється, що загалом зловмисні листи складають 9,3% від загального обсягу пошти, з цього числа 38% містять тільки посилання, а 36% мають вкладення.

Серед месенджерів 90% фішингових атак припадає на WhatsApp, трохи більше 5% — на Telegram.

Посилаючись на інше дослідження від 2022 року, AAG зазначає, що фішингових листів розсилається щоразу більше. З-поміж 1400 опитаних організацій 79% повідомили про зростання числа отриманих листів, зокрема 33% — про суттєве зростання. Особливо тривожно те,що 96% респондентів повідомили про щонайменше одну фішингову атаку вподовж року, і 52% вважають, що ці загрози стали більш вигадливими. 92% вважають, що принаймні одну їхню ділову поштову адресу було скомпрометовано, і 93% зазнали витоку даних через недбальство співробітників або скомпрометовані облікові записи.

Фішинг є основним каналом доставки здирницького ПЗ. Так, у 2021 році дослідники з групи IBM X-Force виявили, що атаки російського угруповання REvil (розформованого у 2022-му) часто починалися з отримання фішингового листа, який містив несплачений рахунок або щось подібне, а в деяких випадках хакери втручалися у листування. Жертва мимоволі встановлювала троянську програму QuackBot, після чого хакери бралися до розвідки і спроб архівації даних. У вищезгаданому опитуванні за участі 1400 організацій серед 26% тих, які повідомили про «значне» зростання загроз, пов'язаних з електронною поштою, 88% стали жертвами кіберздирництва.

Атаки через LinkedIn

Ще одним з трендів фішингу є використання мережі LinkedIn, яка налічує понад 875 млн користувачів у більш ніж 200 країнах. Як пише Ашвін Крішнан з компанії TechTarget (маркетингові послуги для технологічних вендорів), кількість фейкових профілів на платформі LinkedIn невпинно зростає. На перший погляд вони можуть здатися справжніми (містять професійні світлини, переконливі резюме, правдоподібні списки компаній, особисті дані тощо).

Використовуючи фейкові профілі, кіберзлочинці намагаються зв'язатися з обраними жертвами за допомогою прямих повідомлень або запитів на додавання до контактів. Люди, які приймають такі запити, можуть зрештою виказати важливу особисту або службову інформацію. Понад те, отримавши доступ до контактів жертви, злочинець може пробувати завоювати довіру вже цих контактів.

А в міру того, як фальшивий профіль вибудовує власний список контактів, які є реальними користувачами, його позірна легітимність теж зростає.

Іншим варіантом використання LinkedIn є розсилання листів нібито з цієї платформи, щоб обдурити людей, які шукають роботу. За даними AAG, у 1 кварталі 2021 року фішингові листи, відправлені буцімто з LinkedIn, відкривались найчастіше з-поміж усіх листів, що імітували повідомлення від соцмереж (42%; на другому мусці Facebook з 20%, на третьому Twitter з 9%). У 1 кварталі 2022 року 52% усіх ідентифікованих фішингових атак з імітацією брендів соцмереж були саме з LinkedIn.

Ключовими цілями є люди, які полишили своє місце роботи і змінили статус в LinkedIn. Злочинці удають топ-посадовців компаній, намагаючись отримати їхні персональні дані. Інші пропонують купити подарункові ваучери або зателефонувати за вказаним номером, аби обговорити важливі вимоги щодо роботи. Ашвін Крішнан пише, що такі листи містять переконливу символіку LinlkedIn і зміст на кшталт: «Минулого тижня ви з'являлись у 200 пошукових запитах. Натисніть, щоб бути з ними на зв'язку». Проте, перейшовши за посиланням, користувач не потрапить на LinkedIn, а завантажить троян або опиниться на фальшивій сторінці для введення логіна і пароля.

Можливий і комбінований сценарій, коли злочинець, успішно сконтактувавши з жертвою через фейковий профіль, потім для продовження спілкування надсилає листа. Цей лист може містити фішингове посилання або шкідливе ПЗ.

Найочевидніший спосіб вберегтися від такого лиха — взагалі з обережністю приймати запити від незнайомців і уважно придивлятися до профілів, які набиваються в друзі. Якщо сторінка порожня, містить фальшиві імена або імітує публічного діяча, це вже очевидний сигнал. Корисно перевірити фото з профілю — наприклад, за допомогою Google, — щоб дізнатись, чи не вкрадене воно (хоча якщо фото згенероване ШІ, пошук його не покаже).

У 2018 році LinkedIn запровадив автоматизовану систему боротьби з фейковими сторінками, яка складається з кількох ліній оборони. Насамперед модель машинного навчання визначає групи сторінок, схожих за своїм виглядом та поведінкою, тобто вочевидь створених однією особою. Вже створені сторінки групуються за спільними атрибутами, і надалі відстежуються групи, які викликають підозри. Інші моделі відстежують аномальну поведінку серед окремих сторінок або таку, яка є типовою для злочинців. Останнім рубежем оборони є команда людей-розслідувачів.

У 2022 році соцмережа додала можливість перевірки профілю (коли його створено, коли востаннє оновлювався, чи верифіковано робочу поштову адресу тощо). Також LinkedIn попереджає користувачів про «високоризиковий контент» (наприклад, посилання на месенджер або пошту).

Компрометація ділової пошти

Цей вид фішингу є чи не найнебезпечнішим і водночас найбільш дохідним для інтернет-злочинців. AAG наводить дані американського ФБР, згідно з якими у 2020 році шахраї таким чином видурили в організацій сукупно майже $1,9 млрд. Proofpoint повідомляє, що глобально у керівництва компаній найбільшу стурбованість викликає саме BEC (цей злочин назвали 41% респондентів). За підрахунками компанії Cloudflare, у 2021 році на BEC припадало лише 1,3% усіх кібератак з використанням пошти і ще менший відсоток від загальної кількості листів. Проте такі атаки дуже складно виявити, тому що листи не містять ні інфікованих вкладень, ні шкідливих посилань. Практично неможливо і розпізнати підроблений текст.

Для вчинення BEC-атаки злочинці викрадають адреси електронної пошти працівників компаній. Для цього, зокрема, може використовуватись той самий LinkedIn. Після цього вони пишуть працівникам, які мають повноваження вирішувати фінансові питання, але не лише.

ФБР визначає 5 типів схем BEC. По-перше, це імітація топ-посадовця: у цьому разі хакери справді від імені, наприклад, CEO дають розпорядження бухгалтерії щодо переказу коштів на вказаний ними рахунок. Компрометація облікового запису — це злам працівника компанії, з чиєї поштової адреси потім відправляється запит щодо платежу сторонній організації; гроші, ясна річ, перераховуються на рахунок хакера. Виставлення фальшивих рахунків — це, навпаки, коли від імені постачальника хакери надсилають фальшиві реквізити для перерахування грошей. Імітація адвоката відбувається, коли хакер удає юридичного працівника і звертається поштою або телефоном до співробітника нижчої ланки, який може не мати достатнього досвіду або знань, що поставити під сумнів терміновий запит. Викрадення даних — тут зазвичай ціллю є HR-відділ, де хакери отримують інформацію про CEO та інших топ-посадовців, аби в подальшому атакувати вже їх.

Атаки з виставленням фальшивих рахунків можуть бути особливо

Рис. 2. Послідовність BEC-атаки з виставленням фальшивого рахунку (джерело: Armorblox)

підступними. У цьому сценарії (**рис. 2**) хакер зламує пошту одного чи кількох працівників (за допомогою простого фішингу), заходить з іншої IP-адреси і налаштовує автоматичне перенаправлення вхідних листів на спеціально створену скриньку. Після цього хакер читає всі листи і знайомиться з порядками в організації, одночасно він реєструє фейковий домен, що імітує її назву. Якщо в якийсь момент на пошту працівника надходить рахунок, хакер відсилає в бухгалтерію від імені працівника нові платіжні реквізити.

Як зазначає Лорін Кеш з компанії Armorblox (у складі Cisco), такі атаки часто бувають успішними, бо хакер не є стороною, яка подає запит на перерахунок коштів, він лише втручається в існуюче листування, що є менш підозрілим. По-друге, дослідивши роботу організації, хакер знатиме, як вписатися в внутрішні процедури, щоб не бути виявленим. По-третє, у звичайній фішинговій кампанії посадовець, відповідальний за фінансові операції, може сидіти в одній кімнаті з жертвою зламу, що спричинить негайне викриття схеми. Тут же імітують представника стороннього постачальника, зустріч з яким малоймовірна.

Телефонне шахрайство

Серед тенденцій фішингу минулого року Proofpoint ще відзначає поширення атак з доставкою на телефон (telephone-oriented attack delivery — TOAD). У цьому сценарії жертва отримує голосове повідомлення, яке часто містить фальшиве попередження і номер служби підтримки, куди можна звертатись у разі виникнення питань. Якщо користувач зателефонує за таким номером, йому відповість «консультант» (насправді хакер), який запропонує, наприклад, завантажити (зловмисну) програму, перерахувати гроші або відкрити віддалений доступ. Відколи ця техніка з'явилась у 2021 році, кількість випадків постійно зростає, і торік на піку фіксувалось понад 600 тис. TOAD-повідомлень у день.

TOAD — це, по суті, вішинг, який використовується для поширення зловмисного ПЗ. У жовтні 2022 року нідерландська компанія Threat Fabric повідомила про тактику, яка набуває популярності серед злочинців, а саме було розкрито мережу фішингових сайтів, націлених на італійських користувачів онлайн-банкінгу, і встановлено зв'язок між цими сайтами і банківським трояном для Android, що отримав назву Copybara.

Злочинці створили різноманітні фішингові сайти, які імітували сторінки італійських банків і органів кіберзахисту. Усі вони запитували схожий набір персональних даних: номер рахунку, PIN, телефонний номер. У деяких випадках злочинці навіть просили жертв створити секретне питання і відповідь, які мали використовуватись як другий фактор автентифікації. Після цього жертвам повідомляли, що невдовзі з ними зв'яжеться оператор, що й відбувалося з використанням вказаного номера. Оператор «допомагав» жертвам встановити необхідний «захисний» застосунок (**рис. 3**), який насправді є трояном для віддаленого доступу.

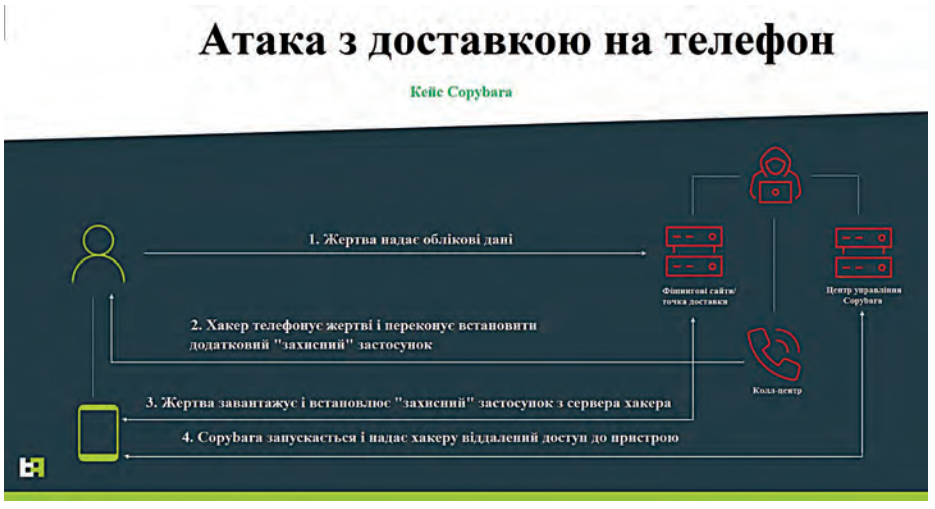

Рис. **3** Алгоритм TOAD-атаки з використанням трояна Copibara (джерело: Threat Fabric)

Завдяки цьому трояну злочинці могли відкривати програми і встановлювати нові, робити кліки і свайпи, вводити дані в поля. Також вони могли видаляти оригінальний банківський застосунок, щоб ускладнити виявлення. Пізніше з'явилась можливість динамічно створювати форми з полями і чекбоксами, щоб отримувати від користувачів ще більше даних.

Подальше розслідування показало, що хакери встановлюють і інші шкідливі програми. Зокрема, один з троянів призначався для крадіжки вхідних SMS, які пересилалися на сервер злочинців. Таким чином останні мали змогу зареєструватися «на новому пристрої», перехопивши одноразовий пароль для авторизації входу.

Передові технології і здорова параноя

То як вберегтися від фішингу? Для цього потрібне поєднання технічних рішень і простого здорового глузду.

Що стосується технологій для протидії фішингу, то тут насамперед мова про захист електронної пошти. ***Gartner*** виділяє три типи таких рішень. По-перше, захищені поштові шлюзи (***SEG***) — традиційні системи, які контролюють вхідний і вихідний трафік і можуть мати вигляд фізичного або віртуального пристрою чи хмарного сервісу. Шлюзи виконують базовий набір функцій захисту, таких як антивірус, пісочниця, карантин спаму, захист від BEC і видалення вже доставлених листів. Для вихідної пошти набір можливостей включає запобігання витокам чутливої інформації, шифрування і відправлення повідомлень через захищений портал. Десятку репрезентативних виробників склали Barracuda, Broadcom (Symantec), Cisco, Fortinet, Microsoft, Mimecast, Proofpoint, Sophos, Trellix і Trend Micro.

По-друге, інтегрований захист хмарної пошти (***ICES***), який доповнює вбудовані функції захисту, що їх надають провайдери хмарних поштових сервісів, такі як Microsoft і Google. ICES

покликаний боротися з більш складними сучасними загрозами і не лише блокує відомий шкідливий контент, а й визначає скомпрометовані облікові записи шляхом аналізу поведінки користувачів (час і місце входу в пошту, метод автентифікації тощо). ICES сповіщає про злам рахунку і може вживати заходів протидії (блокування, скидання паролю і т.ін.). Також ICES може мати механізм сповіщення про фішингові листи з боку користувача. ICES може працювати як на пре-доставці, перехоплюючи листи до того, як вони потраплять до поштової скриньки, так і на пост-доставці, у цьому випадку листи аналізуються постфактум, але можуть приховуватися на час оброблення.

Третій вид рішень — захист поштових даних (***EDP***), тобто різні механізми убезпечення від витоків, зокрема за допомогою шифрування. Деякі рішення також використовують штучний інтелект для визначення листів, які користувач випадково відправляє за хибною адресою.

Forrester у своєму дослідженні систем захисту корпоративної пошти за другий квартал цього року віщує настання золотої епохи після стагнації, яка тривала більшу частину десятиліття. Новими чинниками є масова міграція користувачів до хмарних поштових сервісів, стрімке поширення машинного навчання і повсюдне використання інтерфейсів API для сполучення різних систем і обміну даними. Як результат користувачі отримали змогу комбінувати продукти від кількох виробників або ж поєднувати апаратний шлюз з хмарним сервісом захисту пошти, який ловитиме «те, що просочилося». З іншого боку, поки що мало вендорів приділяють увагу охопленню інших каналів комунікацій, таких як месенджери, засоби спільної роботи і обміну файлами, корпоративні застосунки.

Загалом Forrester, який оцінює виробників за критеріями нинішньої пропозиції, стратегії і ринкової присутності, відносить до лідерів компанії Proofpoint, Microsoft, Check Point і Cloudflare. Біля лідерської межі серед «сильних гравців» розташувались Trend Micro і Google.

Повертаючись до захисту від фішингових атак типу BEC: для їх виявлення виробники використовують цілий арсенал функцій. По-перше, це структурний аналіз листа (тема, адреса вкладення, посилання тощо). Наприклад, перевірка може виявити, що лист відправлено з незахищеного домена, а адреса в підписі стоїть адреса публічного поштового сервісу. Модель машинного навчання з розумінням природної мови (NLU) аналізує вміст листа, розраховує, чи відповідає стиль написання і чи відповідає патерну гаданого відправника, визначає тон листа, шукає спонукальну лексику і ключові слова (наприклад, «платіж», «терміново»).

Фахівці радять (втім, як і скрізь) запроваджувати багатофакторну автентифікацію, принаймні для керівників, адміністраторів, працівників, що мають повноваження проводити платежі, і відділу кадрів.

Технології технологіями, але й розслаблятися не варто. Зловмисники розраховують на те, що жертви спершу діють, а потім думають, і що вони надто заклопотані, щоб розглядати листи критично. Тому фахівці закликають читати вхідні листи дуже обачно. Зокрема скептично ставитися до прохань терміново перерахувати гроші, особливо без належної авторизації, або переслати важливу інформацію. Стерегтися незвичних запитів щодо купівлі чогось, навіть якщо вони надходять від начальства або колег, яким довіряєш. Окремо перевіряти нові реквізити рахунків, які присилають вендори. Обережно ставитись до прохань зберігати все в таємниці та прохань оминути традиційні канали зв'язку. Адже, як відомо, береженого Бог береже.

Василь ТКАЧЕНКО, **МтБ**