



Дмитро ПЕРЕПВА,
вчитель математики та інформатики гімназії №1
Шепетівської міської ради

Соціальна інженерія та фішинг: як навчити школярів розпізнавати цифрові пастки

Сучасна школа існує в умовах постійної цифрової взаємодії. Учні щодня користуються освітніми платформами, електронною поштою, месенджерами, соціальними мережами, хмарними сховищами, сайтами для дистанційного навчання та різноманітними онлайн-сервісами. Для вчителя інформатики таке середовище відкриває широкі можливості для навчання, однак одночасно створює нові загрози, пов'язані з безпекою особистих даних, облікових записів і цифрової репутації. Однією з найнебезпечніших груп ризиків є соціальна інженерія та фішинг, оскільки вони спрямовані не стільки на техніку, скільки на людину, її емоції, довіру, поспіх і неуважність.

Особлива складність цієї проблеми полягає в тому, що школярі часто сприймають цифровий простір як природне продовження повсякденного життя. Вони швидко реагують на повідомлення, охоче переходять за посиланнями, звикають довіряти знайомим аватаркам та назві чату і не завжди замислюються над тим, хто насправді стоїть за екраном. Саме тому навчання дітей правилам безпечної поведінки в мережі має стати системною частиною сучасної інформатичної освіти. Учитель у цьому процесі виконує не лише роль джерела знань, а й роль наставника, який формує уважність, критичне мислення та цифрову відповідальність.

Соціальною інженерією називають сукупність прийомів психологічного впливу, за допомогою яких зломисник спонукає людину добровільно повідомити конфіденційну інформацію, виконати небезпечну дію або надати доступ до ресурсу. На відміну від технічної атаки, де основний акцент робиться на вразливостях програмного забезпечення, у соціальній інженерії ключовою мішенню стає поведінка людини. Зломисник може видавати себе за адміністратора сайту, представника банку, класного керівника, друга, працівника служби підтримки або навіть за автоматичну систему перевірки, щоб викликати довіру і добитися потрібної реакції.

Фішинг є одним із найпоширеніших проявів соціальної інженерії. Його суть полягає в тому, щоб обманом змусити користувача перейти на підроблений сайт, ввести логін і пароль, повідомити код підтвердження, номер телефону, банківські реквізити або інші чутливі відомості. Фішингові повідомлення можуть надходити електронною поштою, через месенджери, соціальні мережі, коментарі під дописами, рекламні банери чи навіть у вигляді спливаючих вікон на звичайних сайтах. Для дітей такі повідомлення часто маскуються під оголошення про подарунок, бонус у грі, результати конкурсу, термінову перевірку акаунта або доступ до нібито важливого навчального матеріалу.

Школярі є особливо вразливою аудиторією для таких маніпуляцій з кількох причин. Передусім у більшості дітей

ще не сформована звичка перевіряти джерело інформації та аналізувати цифровий контент на достовірність. Багато хто діє імпульсивно, спираючись на цікавість або емоцію, а не на перевірку фактів. Додатковим фактором ризику є бажання бути швидкими, не відставати від однолітків, першими отримати новину, знижку чи ігрову перевагу. Усе це робить підлітка легкою мішенню для маніпулятора, який навмисно створює ситуацію поспіху, дефіциту часу або удаваної нагороди.

Не менш важливим чинником є те, що багато дітей не усвідомлюють справжньої цінності власних даних. Для них пароль від електронної пошти, доступ до шкільного облікового запису чи номер телефону можуть здаватися дрібницею, яка не потребує особливого захисту. Насправді ж навіть одна вкрадена комбінація логіна і пароля може відкрити доступ до навчальної платформи, особистого листування, хмарного диска, фотоархіву або інших сервісів, де зберігається приватна інформація. Крім того, компрометація акаунта одного учня нерідко стає джерелом ризику для всього класу, оскільки через знайомий контакт шахраї можуть поширювати нові шкідливі повідомлення.

У шкільному середовищі фішинг набуває особливо небезпечних форм, тому що зломисники можуть паразитувати на авторитеті вчителя, адміністрації закладу чи популярної освітньої платформи. Наприклад, учневі може надійти повідомлення із закликом терміново підтвердити доступ до електронного щоденника, інакше його акаунт буде заблоковано. Інший варіант – лист із нібито посиланням на домашнє завдання, підсумковий тест або результати олімпіади. Дитина, яка звикла довіряти шкільній інформації, часто некритично сприймає таке звернення, надто якщо воно оформлене в переконливому стилі, містить знайомі назви або посилається на відоме їй середовище навчання.

Щоб ефективно протидіяти подібним загрозам, учням потрібно вміти розпізнавати ознаки фішингових повідомлень. Однією з найхарактерніших ознак є навмисне створення відчуття терміновості. У тексті часто наголошується, що акаунт буде заблоковано, доступ втрачено, приз згорить, повідомлення слід відкрити негайно або відповідь треба дати протягом кількох хвилин. Така тактика знижує рівень критичного мислення і спонукає діяти без перевірки. Учитель має систематично звертати увагу дітей на те, що справді важлива офіційна інформація зазвичай не вимагає панічної миттєвої реакції.

Іншою поширеною ознакою є звернення до емоцій. Шахраї можуть використовувати страх, цікавість, жадібність, співчуття або бажання виділитися. Учень може побачити фразу про виграний смартфон, безкоштовний преміум-доступ, секретні відповіді до контрольної, компрометуюче відео або попередження про нібито небезпечну

активність у профілі. У кожному з цих випадків метою є не інформування, а провокування сильного емоційного імпульсу, який зменшує обережність. Тому одна з базових навичок кібергігієни полягає в тому, щоб не виконувати жодних дій під впливом різкого емоційного тиску.

Окрему увагу необхідно приділяти підозрілим повідомленням. Діти мають навчитися помічати відмінність між справжньою адресою сайту і схожою на неї підробкою. Досить часто шахраї використовують зайві символи, помилки в написанні, дефіси, заміну окремих букв цифрами або інші візуально подібні елементи. Навіть якщо сторінка зовні нагадує знайомий сервіс, це ще не свідчить про її справжність. На уроках інформатики доцільно тренувати вміння уважно читати адресу, звертати увагу на домен, аналізувати структуру посилання і не відкривати його автоматично лише тому, що воно надійшло від знайомого контакту.

Ще однією тривожною ознакою є прохання ввести пароль, код із повідомлення, резервний код доступу або інші конфіденційні дані поза звичним середовищем. Учні повинні чітко засвоїти правило: справжній учитель, адміністратор школи чи представник сервісу ніколи не просить надсилати пароль у чаті чи повідомленні. Якщо хтось вимагає такі дані, це привід негайно зупинитися і порадитися з дорослим. Формування саме таких простих, але принципових орієнтирів часто виявляється ефективнішим за надто складні теоретичні пояснення, бо дитина запам'ятовує конкретне правило поведінки.

Про небезпеку можуть свідчити й мовні ознаки повідомлення. Фішингові тексти нерідко містять дивні звороти, невластивий стиль, орфографічні та пунктуаційні помилки, машинний переклад, надмірну офіційність або, навпаки, неприродно фамільярний тон. Іноді повідомлення надсилається від імені знайомої особи, але його зміст не відповідає звичній манері спілкування цієї людини. Такі деталі часто сприймаються як дрібниці, однак саме вони допомагають часом помітити обман. У роботі з учнями корисно не лише називати ці ознаки, а й пропонувати їм самостійно аналізувати приклади та пояснювати, що саме викликає підозру.

Наслідки фішингу для дитини можуть бути значно серйознішими, ніж здається на перший погляд. Це не лише втрата доступу до окремого акаунта. Після захоплення облікового запису шахраї можуть відправляти повідомлення від імені учня, змінювати пароль, отримувати доступ до приватних фото, листування, навчальних документів та списку контактів. Іноді зловмисники намагаються використати скомпрометований акаунт для шантажу, виманювання грошей у батьків чи друзів або для подальшого поширення шкідливих посилань. Таким чином, проблема виходить за межі технічного інциденту і перетворюється на питання безпеки, довіри й психологічного благополуччя.

Для школи подібні випадки також створюють комплекс ризиків. Якщо зловмисники отримують доступ до учнівських або вчительських акаунтів, може бути скомпрометовано освітню платформу, шкільний чат, електронний журнал, хмарний простір для спільних матеріалів або внутрішнє листування. Фальшиві повідомлення від імені педагога здатні викликати паніку, поширити дезінформацію, зірвати виконання завдань або підірвати довіру до цифрових каналів комунікації. У сучасних умовах, коли значна частина навчальної взаємодії відбувається онлайн, навіть один успішний випадок фішингу може мати наслідки для організації освітнього процесу загалом.

Саме тому уроки інформатики мають надавати учням не тільки технічні знання про комп'ютер, файли чи алгоритми, а й практичні інструменти безпечної цифрової поведінки. Формування кібергігієни не повинно зводитися до одноразової бесіди до Дня безпечного інтернету. Значно ефективніше, коли елементи цієї теми системно інтегруються у різні заняття: під час вивчення браузера, електронної пошти, хмарних сервісів, мережевої взаємодії, роботи з обліковими записами, комунікації в інтернеті та основ інформаційної безпеки. Так учні поступово засвоюють, що безпека - це не окремий додаток до цифрової діяльності, а її невід'ємна умова.

Важливим завданням учителя є розвиток критичного мислення. Учень повинен навчитися не просто користуватися сервісом, а ставити запитання: хто є джерелом повідомлення, чи можна йому довіряти, навіщо від мене вимагають цю дію, які наслідки вона може мати, чи є спосіб перевірити інформацію іншим шляхом. Такі запитання корисно багаторазово відпрацьовувати в різних навчальних ситуаціях. Коли дитина починає автоматично зупинятися й аналізувати обставини, шанс успіху маніпулятора помітно зменшується. Отже, цифрова безпека прямо пов'язана з навичкою мислити повільно, уважно і відповідально.

Ефективним методом навчання є розбір конкретних ситуацій, максимально наближених до реального життя школяра. Наприклад, можна запропонувати учням кілька повідомлень і попросити визначити, які з них є безпечними, а які містять ознаки фішингу. Одне повідомлення може імітувати звернення від адміністратора гри, інше - посилання на додатковий матеріал до уроку, третє - нібито подарунок від мобільного оператора, четверте - вимогу терміново відновити пароль. Така вправа корисна тим, що змушує дитину не просто згадувати правило, а застосовувати його в ситуації вибору, порівнювати ознаки та аргументувати власне рішення.

Не менш результативною є рольова модель навчання. Частина класу можна умовно поставити на місце відправника повідомлення і запропонувати визначити, на які почуття він намагається вплинути, якими словами викликає довіру, який гачок використовує для натискання на посилання. Інша частина класу аналізує, як правильно відповісти або що потрібно зробити, щоб уникнути ризику. Подібний формат дає змогу побачити механізм маніпуляції зсередини, а отже, краще його розуміти. Учні починають усвідомлювати, що небезпека часто ховається не у складних програмах, а в добре продуманому сценарії психологічного впливу.

Доречними є й короткі алгоритми безпечної реакції, сформульовані в доступній для дітей формі. Передусім потрібно зупинитися і не діяти одразу. Далі - уважно прочитати повідомлення, перевірити адресу відправника або посилання, пригадати, чи очікувалось таке звернення, не вводити пароль та не надсилати коди підтвердження. Якщо зміст викликає сумнів, варто звернутися до вчителя, батьків або адміністратора платформи через офіційний канал. Коли такі дії неодноразово відпрацьовуються на практиці, вони поступово стають звичкою, а не випадковою реакцією.

Особливо корисно поєднувати тему фішингу з навчанням створення надійних паролів і використання двоетапної перевірки. Учні мають зрозуміти, що один пароль для всіх сервісів є небезпечною практикою, а доступ до пошти часто є ключем до відновлення інших облікових записів. Якщо дитина використовує різні складні паролі та додатковий фактор під-

твердження, навіть успішна спроба виманити дані не завжди призведе до повного захоплення цифрового середовища. Такий зв'язок між окремими правилами кібергігієни допомагає сформувати цілісне уявлення про особисту цифрову безпеку.

Окремий напрям педагогічної роботи пов'язаний із формуванням відповідального ставлення до поширення інформації. Учні нерідко пересилають повідомлення друзям ще до того, як замисляться над їхнім змістом. Саме так фішингові посилання часто швидко розходяться класними чатами або приватними діалогами. Важливо пояснювати дітям, що пересилання підозрілого повідомлення робить їх несвідомими учасниками ланцюга маніпуляції. Отже, безпечна поведінка в мережі включає не лише вміння захистити себе, а й відповідальність не створювати загрози для інших учасників спільноти.

У роботі з молодшими школярами доцільно використовувати простіші формулювання і наочні приклади. Для них можна запропонувати правило трьох запитань: хто це надіслав, що від мене хочуть, чи можна спитати дорослого. У середніх і старших класах доречно ускладнювати зміст, вводити поняття соціальної інженерії, цифрового сліду, багатофакторного захисту, аналізувати реалістичні сценарії, обговорювати фейкові сайти та підроблені сторінки входу. Така вікова диференціація робить навчання не формальним, а справді результативним, оскільки відповідає рівню досвіду і когнітивним можливостям учнів.

Практика показує, що діти краще запам'ятовують не сухі визначення, а історії та ситуації, у яких можна впізнати себе. Саме тому корисно використовувати навчальні кейси, наближені до їхнього повсякденного життя. Це можуть бути приклади з ігрових платформ, соцмереж, шкільних чатів, сайтів конкурсів, сервісів для реєстрації або отримання навчальних матеріалів. Коли учень бачить знайоме середовище, він легше переносить вивчене правило в реальну поведінку. У результаті статичне знання перетворюється на дієву навичку, а це і є головною метою навчання безпечного користування цифровими ресурсами.

Корисним інструментом може стати створення спільної пам'ятки класу або школи з короткими правилами протидії цифровим пасткам. Учні можуть разом із учителем сформулювати, які повідомлення слід вважати підозрілими, чому не можна повідомляти паролі, як перевіряти посилання, до кого звертатися по допомогу і що робити у випадку, якщо хтось уже натиснув на небезпечний ресурс. Така пам'ятка виконує не лише інформаційну, а й виховну функцію, оскільки створює в колективі спільне розуміння норм безпечної поведінки та спонукає дітей відчувати відповідальність за власні дії в мережі.

Учителю інформатики важливо також звертати увагу на мовленнєву сторону цифрової безпеки. Діти мають навчитися коректно описувати проблему: не просто казати, що сайт дивний, а пояснювати, які саме ознаки викликали сумнів; не просто відчувати небезпеку, а вміти аргументувати її. Такий підхід допомагає перевести інтуїтивне враження в усвідомлене судження. Коли учень може словами назвати ознаки маніпуляції, він краще контролює власну поведінку і в майбутньому легше передає це знання іншим. Отже, робота з кібербезпекою сприяє також розвитку мовлення, логіки та культури аргументації.

Не варто забувати і про роль батьків. Навіть найзмістовніший урок не забезпечить належного результату, якщо вдома дитина залишається наодинці з ризиками, не має звички радитися з дорослими і не відчуває підтрим-

ки. Батькам важливо пояснювати, що цифрова безпека починається не з заборон, а з довірливого спілкування. Дитина має знати, що якщо вона випадково перейшла за підозрілим посиланням або повідомила зайву інформацію, її не будуть одразу сварити, а допоможуть виправити ситуацію. Саме атмосфера довіри збільшує ймовірність того, що проблему буде виявлено вчасно.

Співпраця школи і родини може відбуватися у формі коротких інформаційних повідомлень, тематичних батьківських зборів, пам'яток, консультацій або спільних правил користування пристроями. Доцільно наголошувати батькам, що діти мають право на навчання в цифровому середовищі, але це середовище потребує такої ж уваги до безпеки, як і реальне життя. Якщо дорослі самі ігнорують елементарні правила, використовують ненадійні паролі або бездумно переходять за посиланнями, переконати дитину в цінності кібергігієни буде складно. Тому профілактика фішингу є спільною відповідальністю всіх учасників освітнього процесу.

Не менш важливим є питання педагогічного тону під час вивчення теми. Якщо подавати фішинг і соціальну інженерію лише як перелік страшних загроз, можна сформувати в дітей не обережність, а тривожність або безпорадність. Значно продуктивніше показувати, що більшість цифрових пасток можна розпізнати, якщо знати їхні ознаки і діяти спокійно. Учень повинен винести з уроку не страх перед інтернетом, а впевненість у тому, що він має інструменти для захисту. Такий підхід сприяє не лише безпеці, а й формуванню зрілої, відповідальної та самостійної цифрової особистості.

У професійній діяльності вчителя ця тема також має практичний вимір. Педагог, який сам дотримується правил кібергігієни, стає для учнів переконливим прикладом. Якщо вчитель перевіряє джерела, обережно ставиться до листів, використовує надійні паролі, не пересилає сумнівний контент і пояснює свої дії, діти сприймають таку поведінку як норму. Натомість формальні зауваження без особистого прикладу мають значно менший вплив. Отже, навчання безпечної поведінки в мережі нерозривно пов'язане з цифровою культурою самого педагога та загальною культурою комунікації в закладі освіти.

Проблема фішингу особливо актуалізується в періоди активного використання дистанційних або змішаних форм навчання. Саме тоді кількість електронних повідомлень, навчальних посилань, реєстрацій, кодів доступу і термінових повідомлень різко зростає. На цьому тлі дітям важче відрізнити справжню комунікацію від підробленої. Зловмисники добре розуміють цю особливість і часто маскують свої дії під навчальну активність. Що більше школа використовує цифрові засоби, то вагомішим стає завдання навчити учнів не лише користуватися платформою, а й безпечно орієнтуватися в інформаційному потоці.

Важливим аспектом є й те, що цифрова безпека не може бути засвоєна раз і назавжди у вигляді набору готових відповідей. Змінюються сервіси, формати повідомлень, зовнішній вигляд платформ, стилі комунікації. Проте незмінними залишаються базові принципи: не поспішати, перевіряти джерело, не розкривати конфіденційні дані, сумніватися в надто вигідних або надто тривожних повідомленнях, звертатися по допомогу у випадку невпевненості. Якщо навчання будується саме на цих принципах, то учень зможе застосувати їх і до нових ситуацій, з якими він ще не стикався безпосередньо на уроці.