3. Звертайте увагу на адресний рядок: незначні зміни в електронній адресі можуть привести вас на абсолютно інший сайт (наприклад, замість mail.ru може бути meil.ru, а замість vk.com - vk.co або vka.com).
4. При відвідуванні банківських сайтів, стежте, щоб було встановлене захищене з'єднання https.
5. Листи з невідомих адрес, які «тиснуть на емоції» або носять екстрений характер, повинні в першу чергу викликати підозри. Листи, які починаються з таких заяв, як «Ваш профіль буде заблоковано!» Або, навпаки, оголошують вам про великий виграш, в більшості випадків є шахрайськими.
6. Будьте обережні заходячи на банківські веб-акаунти через точки доступу громадського Wi-Fi.
7. Якщо виявили фішинговий лист нібито від відомої вам компанії або сервісу, повідомте про це у відділення цієї компанії.

Не так давно одна з британських компаній, що спеціалізується на захисті від шахрайства в інтернеті, провела цікавий експеримент. Відвідувачам кав'ярні пропонували безкоштовну каву в обмін на лайк корпоративної сторінки закладу в Facebook. Поки відвідувач робив замовлення, співробітники аналізували профіль людини і дізнавалися про нього безліч особистої інформації. Поки готувалася кава, бариста встигав «вивалити» на приголомшену людину інформацію про його день народження, імена батьків, освіту, віросповідання і тому подібне. І все це завдяки всього-на-всього одного лайку! Таким інтерактивним способом компанія акцентувала увагу громадян на необхідність захисту своїх персональних даних.

Пропонуємо, один із засобів боротьби з фішинговими атаками. AdBlock - це розширення для веб-браузера. Воно не тільки заблокує зайву рекламу, а ще попередить про неперевірені сайти. Adblock блокує HTTP-запити відповідно з адресами джерела і може блокувати різні типи елементів сторінки.

ВИКОРИСТАННЯ SQL-ЗАПИТІВ ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ З СИСТЕМИ MOODLE

Лє В`єт Ань
Науковий керівник – ***Бочаров Б.П., канд. техн. наук, доцент***
(Харківський національний університет міського господарства імені О.М. Бекетова)

В системі дистанційного навчання Харківського національного університету міського господарства встановлено спеціальний модуль

[1], що дозволяє відправляти запити і отримувати інформацію з системи Moodle. Модуль дуже строго перевіряє запити і не дозволяє вживати ключові слова, які змінюють базу даних, в будь-якому контексті.

Як приклад розглянемо запит, що виводить інформацію про перевірки практичних робіт на курсі (update grades). У запиті використовується конструкція «action LIKE '%grades'», тому що слово «update» блокується як небезпечне.

```
SELECT
prefix_log.id,
FROM_UNIXTIME(prefix_log.time) AS 'TIME',
prefix_log.userid,
prefix_log.ip,
prefix_log.course,
prefix_log.module,
prefix_log.cmid,
prefix_log.action,
prefix_log.url,
prefix_log.info
FROM
prefix_log
WHERE
prefix_log.action LIKE '%grades'
AND
(prefix_log.course = 24)
ORDER BY prefix_log.id DESC
```

1. Бочаров Б.П. Інформаційні технології в освіті : монографія / Б.П. Бочаров, М.Ю. Воєводіна; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. – Харків: ХНУМГ ім. О. М. Бекетова, 2015. – 197 с.

КОНЦЕПЦІЯ “LANDING PAGE” ДЛЯ САЙТУ НАВЧАЛЬНОГО ЗАКЛАДУ

Клименко Р.В.
Науковий керівник – ***Бочаров Б.П., канд. техн. наук, доцент***

Landing page (цільова, посадочна сторінка) – це інтернет-сторінка, спрямована на спонукання користувача вчинити будь-яку дію: підписатися на розсилку, купити продукт, скачати софт. У нашому випадку – вступити до Харківського національного університету міського господарства на спеціальності кафедри Прикладної математики та інформаційних технологій.

Виділяють наступні типи Landing page: