Рекомендації щодо виявлення фішингових вебсайтів
та як захиститися від фішингових атак і повідомляти про них

Що таке фішинг?
Фішингова атака – це спроба отримати вашу особисту інформацію оманливим шляхом.

Як працює фішинг?
Фішингові атаки зазвичай здійснюються через електронні листи, оголошення або сайти, схожі на ті, які ви відвідуєте. Наприклад, ви можете отримати електронний лист, схожий на лист із Банку, з проханням підтвердити номер банківського рахунку.
Інформація, яку можуть запитувати фішингові сайти:

- Імена користувача та паролі;
- Номери банківських рахунків;
- PIN-коди (особисті ідентифікаційні номери);
- Номери кредитних карток;
- Дівоче прізвище матері;
- Ваш день народження;

Як уникнути фішингу?
Будьте обережними, коли отримуєте повідомлення від сайту з проханням надати особисту інформацію. Якщо вам надходять такі повідомлення, не надавайте інформацію, не переконавшись у надійності сайту. Якщо можливо, відкрийте сторінку в іншому вікні, а не натискайте посилання в електронному листі.

Банк ніколи не надсилатиме небажані повідомлення з проханням повідомити пароль або іншу особисту інформацію.

1. Завжди здійснюйте візуальну перевірку доменного імені для переконання, що це офіційний сайт Банка, а не фішингова сторінка зловмисників.
2. При підключенні до веб-сайтів Банку перевірте наявність значка «Замок» у вікні браузера, що свідчить про ввімкнене шифрування.
3. Про встановлення безпечного з'єднання між браузером Користувача та сервером Банку свідчить цифровий (електронний) сертифікат. Перевірте надійність надавача, дійсність сертифікату та термін його дії.
4. Забезпечте належний захист платіжної карти під час розрахунків у мережі Інтернет: – здійснюйте онлайн-розрахунки виключно на перевірених сайтах великих Інтернет-магазинів, постачальників послуг тощо та уважно перевіряйте їх адресу.
5. Уважно аналізуйте SMS-повідомлення або повідомлення в месенджерах, що надходять від імені Банку. Переходить за посиланням в повідомленні виключно після того як впевнилися, що повідомлення від Банку.

При виявленні сайту ззовні схожого на сайт АТ «БАНК АВАНГАРД» обов'язково повідомте про це Банк за будь-яким зручним для Вас способом, зазначеним в контактах Банку: https://avgd.ua/contacts/

Українська міжбанківська асоціація членів платіжних систем ЕМА, яка за підтримки Державного департаменту США реалізує в Україні Національну програму сприяння безпеці електронних платежів і карткових розрахунків Safe Card, створила та регулярно оновлює список виявлених фішингових сайтів.

Ознайомитися з переліком сайтів, які становлять небезпеку можна на офіційному сайті ЕМА в розділі «Чорний список сайтів»: https://www.ema.com.ua/citizens/blacklist/

Перелік перевірених надійних платіжних сервісів: https://www.ema.com.ua/citizens/whitelist/

Національний банк України на своєму офіційному Інтернет-представництві розмістив довідник банків, що містить інформацію про банки та відокремлені підрозділи банків України, який розміщено за даним посиланням: https://bank.gov.ua/ua/supervision/institutions/