Безпека розрахунків в мережі Інтернет

Увага! Фішинг – підміна веб-сайтів, веб-ресурсів з метою отримання персональних даних держателя банківської платіжної картки з подальшим проведенням шахрайських операцій в CNP-середовищі та/або синхронно з держателем банківської платіжної картки здійснювати шахрайські операції з переказу з картки на картку через легальний платіжний сервіс, використовуючи дані, які держатель вводить на шахрайському веб-сайті та замінюючи номер картки отримувача та номер картки шахрая, а в деяких випадках збільшуючи суму переказу. Коли держатель вводить карткові реквізити на такому веб-сайті, запит на авторизацію операції до банку надходить, але банк авторизує операцію, яку здійснює злочинець.

Користувач не завжди може помітити, що веб-сайт є підробленим, просто переглядаючи сторінки в мережі Інтернет, оскільки шахраї дуже пильно копіюють реальний вміст популярного веб-сайту.

Щоб уберегтися від фішингу використовуйте прості правила:

- Подивіться на URL-адресу, щоб переконатися, що Ви дійсно перебуваєте на реальному веб-сайті;
- URL-адреса повинна починатися з https: // (не http: //), і Ви повинні бачити логотип веб-безпеки – зелений замочок - в адресному рядку браузера.
- Не переходьте і не оплачуйте послуги за посиланнями, отриманих від незнайомих людей або у SMS-повідомленнях або за скороченими лінками.
- Увага! Повна версія сайту Ідея банку виглядає так - https://ideabank.ua

Будьте обачними та у випадку виявлення недобросовісного веб-сайту або користувача в мережі Інтернет одразу повідомляйте в Кіберполіцію за посиланням - https://ticket.cyberpolice.gov.ua/
Довідник банків які мають банківську ліцензію та їх відокремлених підрозділів - https://bank.gov.ua/ua/supervision/institutions

Під час оплати покупок в Інтернеті необхідно зазначати тільки номер картки, строк дії та CVV2-код. З метою безпеки ніколи не передавайте код CVV2 Вашої картки стороннім особам!

Будьте обережні й не розголошуйте особисті дані. Якщо Вас просять назвати дату та рік народження, дівоче прізвище матері та інші особисті дані або набрати різні комбінації цифр на телефоні, то Ви маєте справу з шахраєм. Якщо Ви часто здійснюєте купівлі в мережі Інтернет, завжди звертайте увагу на інтерфейс сайту для оплати – будь-яка зміна кольорової гами та шрифту, наявність орфографічних помилок має викликати підозри. А ще краще заведіть для цього окрему карту з невеликим лімітом.