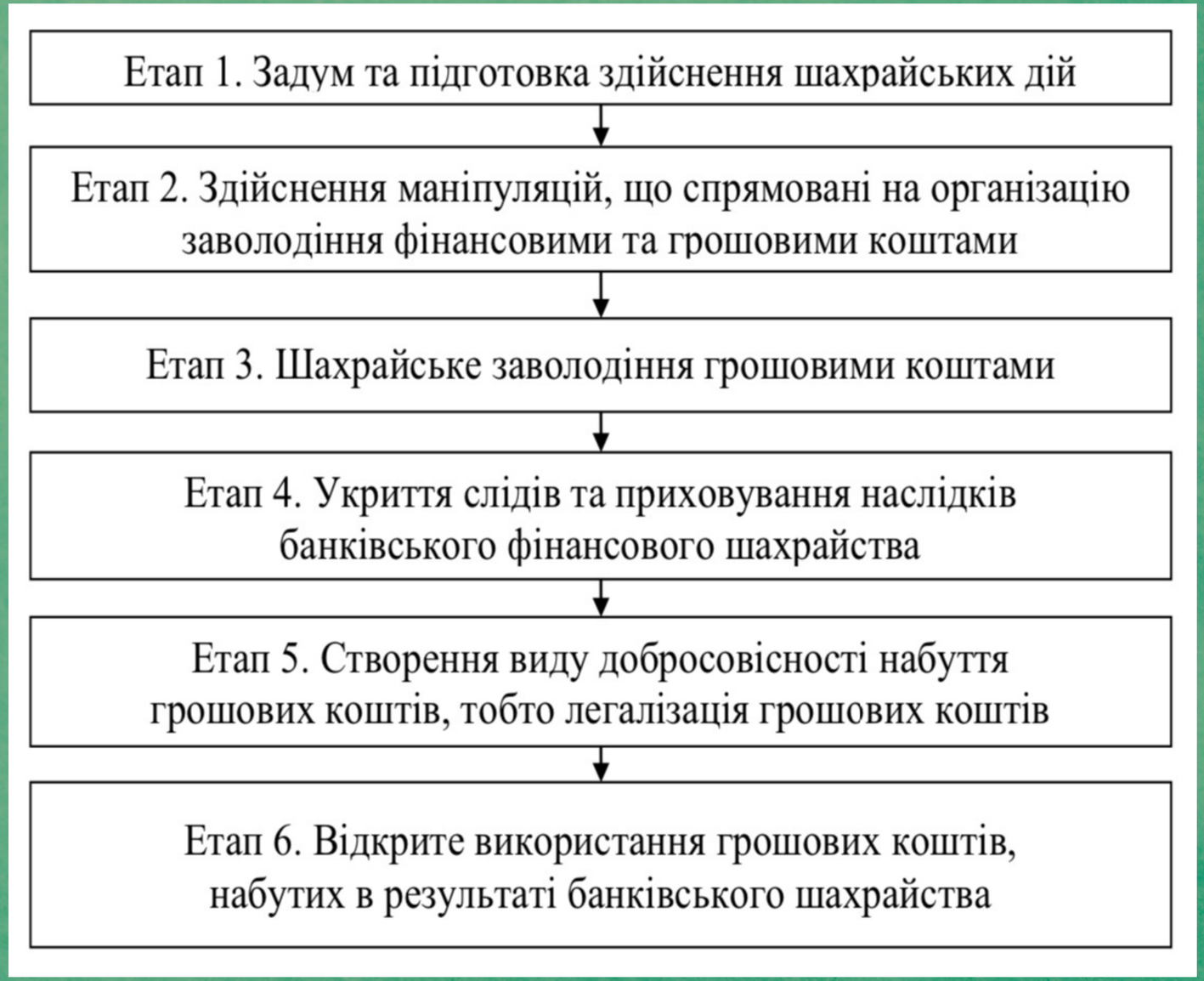
Шахрайства в банківській і фінансовій сфері: загрози і шляхи боротьби

Банківське шахрайство

Банківське шахрайство – це приховуваний процес систематичного ураження фінансової безпеки банку, який призводить до фінансових збитків, втрати довіри та репутації серед клієнтів, а в окремих випадках може стати причиною банкрутства банківської установи.

Схема повного циклу банківського шахрайства



Фінансове шахрайство

Фінансове шахрайство – це злочинна діяльність, що відображає грошові потоки між суб'єктами фінансових відносин, в результаті яких відбувається отримання економічних вигід шахраєм та збитків – жертвою шахрайських дій.

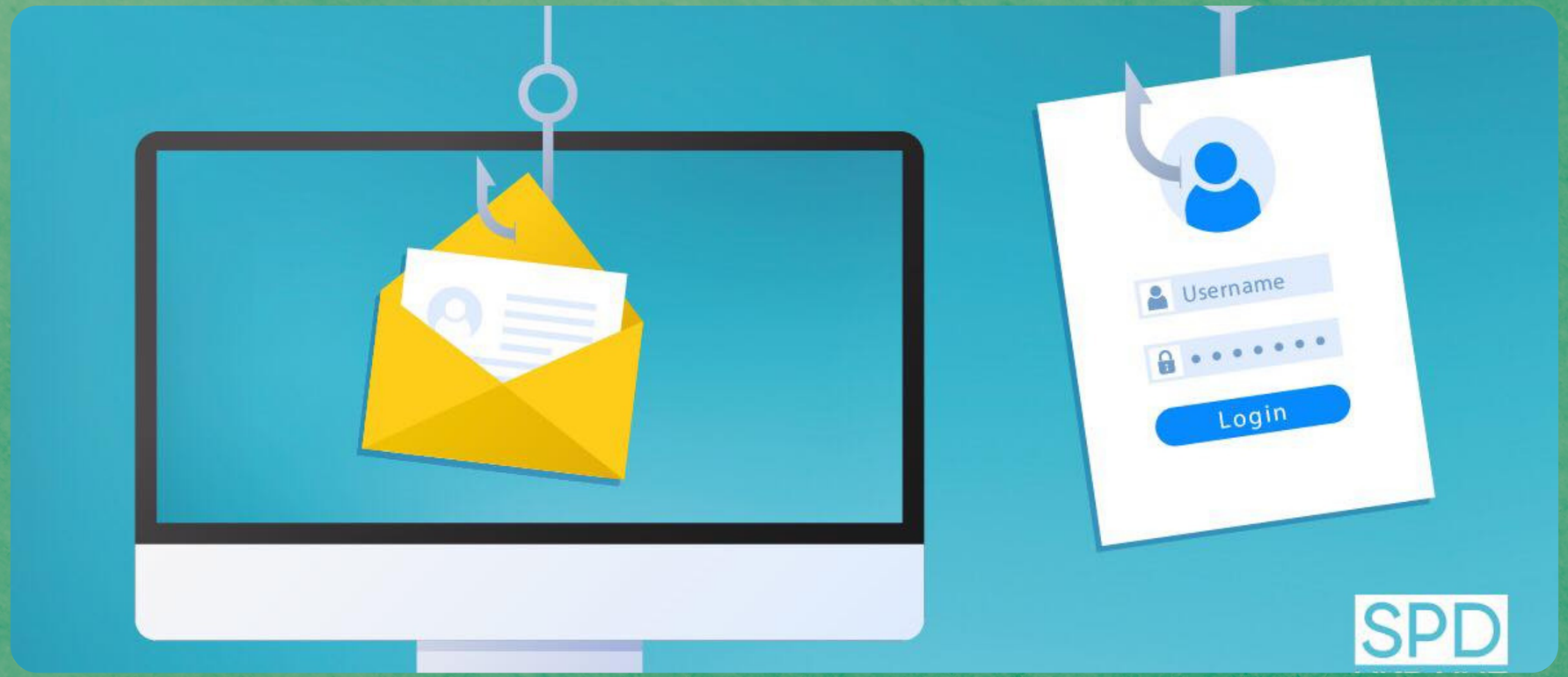
Основними типами шахрайства в Україні залишаються фішинг та соціальна інжинерія, зважаючи на вразливість населення у зв’язку із ситуацією в країні. Їх частка становить майже 80% від усіх видів шахрайства, які фіксуються в інтернет-просторі.

Фішинг

Фішинг – це спосіб виманити в людини дані банківської картки за допомогою інтернет-ресурів. Для цього шахраї створюють копії сайтів банків, інтернет-магазинів чи платіжних систем. Проводячи на таких сайтах оплату, жертва вносить туди свої банківські дані, після чого шахраї отримують доступ до її банківського рахунку.

Шахраї можуть створити не лише копію відомого сайту, а й новий сайт. Часто таким чином створюють інтернет-магазини техніки та гаджетів з привабливими цінами.

Ще один варіант фішингу пов'язаний з використанням служб доставки – "Нової пошти", DHC, "Укрпошти". Жертвам може прийти повідомлення про доставку посилки і необхідність сплатити за неї кошти. Для проведення розрахунків шахраї пропонують перейти за посиланням на фішинговий сайт, який імітує сайт служби доставки.



Історія фішингу почалася у 1995 році, коли у мережі Америка Онлайн (AOL) шахраї почали активно використовувати непоінформованість користувачів для одержання конфіденційних відомостей. Пізніше здивованим співробітникам AOL довелося писати клієнтам листа про те, що AOL ніколи не запитує у своїх клієнтів конфіденційної інформації з пошти. До речі, не запитують аналогічну інформацію також і співробітники банків та платіжних систем.

Кожному користувачеві можна порадити: ніколи не квапитися ділитися конфіденційною інформацією, зверніться до банку і впевніться у тому, що інформація запитується дійсно представником банку та в обґрунтованих цілях.

Соціальний інжиніринг

Соціальний інжиніринг – це складніші схеми: зловмисники намагаються зробити так, аби жертва добровільно переказала їм кошти або назвала конфіденційну банківську інформацію, нічого при цьому не запідозривши. Для цього шахраї можуть втертися в довіру до цієї людини, зокрема видавши себе за знайомого чи родича жертви.

Інколи зловмисники можуть зламати акаунт людини в соцмережах та отримати доступ до її листування. Проаналізувавши діалоги, шахраї обирають близьких та друзів жертви, які можуть погодитися без зайвих запитань надіслати гроші "для вирішення термінової проблеми". Це можуть бути проблеми із здоров’ям або затримання правоохоронцями, тоді злочинці просять гроші нібито на хабар.

Методи протидії шахраям

Ніколи не надавайте інформацію про свої картки третім особам, навіть якщо вони звертаються до вас нібито від імені банку.

Будьте пильні, якщо вам приходять SMS невідомого авторства з проханням надіслати отриманий код або дивний набір команд на інший номер.

Використовуйте багатофакторну автентифікацію (MFA) та систему перевірки адрес (AVS)

Регулярно перевіряйте стан свого рахунку як у платіжній системі, так і на картці. Якщо у вашому банку є послуга СМС-повідомлення – обов'язково підключіть її, тому що це найшвидший спосіб одержати інформацію про те, що з вашим рахунком щось відбувається. У жодному разі не зберігайте всі ваші гроші на банківській картці.

Акуратніше використовуйте та говоріть про інформацію, яка використовується вами для відповіді на друге секретне запитання при відновленні пароля.
Ніколи не здійснюйте операцій по картках за допомогою електронних платіжних систем у магазинах, яким не довіряєте або які бачите вперше. Особливо, якщо на них немає логотипів платіжних систем, та інших організацій, які борються із шахраями.

Не залишайте платіжні картки без догляду й не передавайте третім особам.
Ніколи не повідомляйте CVV/CVC-код нікому, за винятком процесу оплати в Інтернет-магазині, тому що це необхідно для завершення угоди.
У жодному разі не надавайте особисту інформацію у відповідь електронною поштою. Жоден банк і жоден сервіс ніколи не попросять вас надати пароль доступу.

Кучирка Сніжана Володимирівна
Телефон: 0686575183
Адреса електронної пошти:
kuchyrka.snizhana.clg@chnu.edu.u
ВСП «Фаховий коледж ЧНУ імені Юрія Федьковича»