

КІБЕРБЕЗПЕКА

думай швидко,
плати безпечно!

Картки із завданнями
для проведення гри з платіжної
безпеки



#ШахрайГудбай

Картка № 1



1. CVV-код
2. Соціальна інженерія
3. Кіберполіція
4. Афера
5. Індивідуальний ліміт
6. Фішинг
7. Зазначте правило, якого потрібно дотримуватися під час оформлення грошових виплат
8. Наведіть приклад шахрайства із застосуванням технології спуфінг.

Картка № 2



1. Особисті дані
2. Протокол сайту
3. Шахрай
4. Логін
5. Багатофакторна автентифікація
6. Скімінг
7. Яку інформацію про платіжку картку нікому не можна повідомляти?
8. Наведіть приклад смс-шахрайства.

Картка № 3



1. Хакер
2. Злам акаунта
3. Телефонне шахрайство
4. Тримати в секреті пін-код
5. Інтернет-банкінг
6. Перевірка сайту
7. Назвіть пораду, як перевіряти сайт, на якому платите вперше
8. Наведіть приклад будь-якого телефонного шахрайства.

Картка № 4



1. Одноразовий пароль
2. SIM-картка
3. Онлайн-шопінг
4. Заблокувати платіжну картку
5. Фішинговий сайт
6. Дроп
7. Назвіть правило, якого потрібно дотримуватися під час покупок на онлайн-майданчиках
8. Наведіть приклад шахрайства під виглядом грошових виплат.

Картка № 5



1. Фінансовий номер телефону
2. Аферист
3. Психологічний тиск
4. Інтернет-магазин
5. Переказ коштів
6. Передплата
7. Як, крім пароля, можна захистити свій акаунт?
8. Наведіть приклад схеми шахрайства від імені псевдопродавця.

Картка № 6



1. Вірус
2. Спуфінг
3. Післяплата
4. Кодове слово
5. Грошовий мул
6. NFC
7. Назвіть одну пораду, як захистити номер телефону, прив'язаний до банківського рахунку?
8. Наведіть приклад шахрайства від імені "працівника банку".

Картка № 7



1. Обліковий запис
2. Підробка
3. Надійний пароль
4. Псевдопродавець
5. Дезінформація
6. Платіжний термінал
7. Який протокол сайту вважається ненадійним?
8. Наведіть приклад шахрайства під виглядом покупця.

Картка № 8



1. Банківський рахунок
2. Псевдопокупець
3. Платіжна безпека
4. Кібератака
5. Касовий чек
6. VPN
7. Назвіть один лайфхак безпечних онлайн-покупок
8. Наведіть приклад шахрайства в соціальних мережах.

Картка № 9



1. Загальнодоступна мережа Wi-fi
2. Відновлення пароля
3. Платіжна картка
4. Кібергігієна
5. Спам
6. Зняти гроші з картки
7. Назвіть одну пораду, як перевірити сторінку інтернет-магазину в інстаграмі
8. Наведіть приклад шахрайства через смс-повідомлення.

Картка № 10



1. Пароль
2. Антивірус
3. Термін дії картки
4. Схема шахрайства
5. Зловмисники
6. Кіберзагроза
7. Пише друг в соціальних мережах і просить у борг. Як переконалися, що це не шахрай?
8. Наведіть приклад телефонного шахрайства від імені "працівника банку".

Картка № 11



1. Кібербезпека
2. Віртуальна картка
3. Фейковий магазин
4. Банкомат
5. Шахрайське посилання
6. Безпечний платіж
7. Зазначте інформацію, яку не можна використовувати для створення паролів
8. Наведіть приклад телефонного шахрайства від імені "працівника поліції".

Картка № 12



1. Реквізити картки
2. Шахрайський чат-бот
3. Національний банк України
4. Кіберзлочинці
5. Втрата коштів
6. Запобігання шахрайству
7. Що потрібно зробити насамперед, якщо ваш акаунт зламали, але ви ще маєте до нього доступ?
8. Наведіть приклад шахрайства про фейковий виграш.

Картка № 13

1. Ввести ПІН-код
2. Маніпуляція
3. Ліцензійна програма
4. Шахрайське повідомлення
5. Унікальний пароль
6. Онлайн-платежі
7. Назвіть одну пораду, як захисти номер телефону, прив'язаний до банківського рахунку?
8. Наведіть приклад телефонного шахрайства від імені мобільного оператора.



Картка № 14

1. Заблокувати рахунок
2. Стоп фразд
3. ПІН-код
4. Шахрайський кол-центр
5. Створити акаунт
6. Хакерська атака
7. Назвіть одну пораду, як захистити свій смартфон.
8. Наведіть приклад шахрайства у формі збору коштів на благодійність.



Картка № 15

1. Фішингове посилання
2. СМС-код
3. Екран банкомата
4. Шахрайство
5. Face ID
6. Підтвердження платежу
7. Назвіть одну пораду, щоб не потрапити до рук шахраїв під час використання загальнодоступної мережі Wi-Fi
8. Наведіть приклад шахрайства під час оренди житла.

