План гостьової лекції від фахівців АТ УКРСИББАНК: «Платіжна безпека та протидія фінансовому шахрайству»

Мета заходу: підвищити рівень фінансової грамотності молоді, навчити розпізнавати основні види кібершахрайства та ознайомити з інструментами захисту власних коштів.

У результаті участі в гостьовій лекції від фахівців АТ УКРСИББАНК, студенти здобудуть комплекс **загальних та фахових компетенцій**, що базуються на матеріалах Національного банку України та практичному досвіді банківських експертів:

Інформаційно-цифрова компетентність

- **Розпізнавання фішингу:** здатність ідентифікувати шахрайські повідомлення в месенджерах, СМС та електронній пошті, спрямовані на викрадення персональних даних.
- **Навички безпечної навігації:** розуміння ризиків переходу за неперевіреними посиланнями, навіть якщо вони надійшли від знайомих осіб.
- **Кібергігієна пристроїв:** уміння налаштовувати багаторівневий захист смартфона за допомогою паролів та біометричних даних (відбиток пальця, FaceID).
- **Захист конфіденційної інформації:** навички налаштування приватності сповіщень на заблокованому екрані для запобігання витоку банківських кодів.

Фінансова грамотність та безпека

- **Управління платіжними ризиками:** здатність розрізняти публічні дані банківської картки (16-значний номер) від секретних реквізитів (CVV-код, термін дії, ПІН-код).
- **Протидія соціальній інженерії:** уміння виявляти методи психологічного тиску та маніпуляцій під час телефонних розмов із шахраями (вішинг).
- **Фізична безпека розрахунків:** оволодіння технікою безпечного використання банкоматів для захисту від скімінгу.
- **Алгоритм дій у кризових ситуаціях:** чітке розуміння послідовності кроків у разі втрати смартфона або виявлення шахрайства.

Техніко-криптографічна грамотність

- **Створення стійких паролів:** навичка генерації складних комбінацій символів, що не базуються на персональних уподобаннях чи датах народження.
- **Використання мнемонічних методів:** здатність створювати надійні паролі на основі автентичних українських джерел (пісень, прислів'їв), що підвищує рівень захисту облікових записів.

Професійна та кар'єрна компетентність

- **Основи банківської етики:** ознайомлення зі стандартами професійної діяльності працівників банку через безпосередню комунікацію з топменеджментом Подільського департаменту.

- **Готовність до працевлаштування:** отримання сертифікованих знань (Диплом школи Юного банкіра), що засвідчують відповідність сучасним вимогам банківського сектору до компетенцій працівників.

Ці компетенції не лише захищають особисті фінанси студентів, а й формують фундамент їхньої професійної надійності як майбутніх фахівців в економічній сфері.

I. Вступна частина (10 хвилин)

- **Привітання та знайомство:** представлення спікерів від **UKRSIBBANK**.
- **Актуальність теми:** як шахрайство еволюціонувало з реального світу у віртуальний.
- **Статистика та міфи:** розвіювання міфу, що шахраї — це завжди незнайомці (можуть видавати себе за друзів, поліцію або працівників банку).

II. Основна частина: Анатомія шахрайства (45 хвилин)

1. Фішинг — «риболовля» в інтернеті
   - **Методи розповсюдження:** шкідливі посилання в месенджерах, СМС та e-mail.
   - **Кейс «Повідомлення від друга»:** аналіз ситуацій, коли просять позичити гроші або перейти за посиланням «ти на відео?».
   - **Правила безпеки:** принцип «Спочатку думай — потім клікай!».
2. Вішинг — телефонне маніпулювання
   - **На що полює шахрай:** дані картки, паролі, СМС-коди від банку.
   - **Головне правило:** якщо питають секретні дані по телефону — негайно кладіть слухавку та повідомте дорослих/банк.
3. Скімінг — небезпека біля банкомата
   - **Як це працює:** використання прихованих камер та спеціального обладнання на банкоматах.
   - **Практична порада:** як правильно прикривати клавіатуру під час введення ПІН-коду.

III. Практичний блок: Ваш смартфон — ваш цифровий гаманець (20 хвилин)

- **Захист пристрою:** використання біометрії (FaceID, відбиток пальця) та складних паролів.
- **Конфіденційність:** налаштування сповіщень так, щоб їх вміст не було видно на заблокованому екрані.
- **Алгоритм дій при втраті смартфона:** повідомити батьків та змінити всі паролі.

IV. Майстер-клас зі створення паролів (10 хвилин)

- **Що НЕ використовувати:** імена тварин, дати народження, прості комбінації.
- **Метод «Українська автентичність»:** створення паролів на основі рядків з пісень, віршів або мотиваційних фраз.

- *Приклад:* «Ой у лузі червона калина...».

V. Закріплення матеріалу

- **Інтерактивний квіз «Детектор шахрайства»:** Викладач зачитує реальні тексти СМС або сценарії дзвінків, а студенти мають підняти червону картку («Шахрай!») або зелену («Безпечно»). Це допомагає миттєво розпізнати ознаки фішингу та вішингу.
- **Аналіз платіжної картки:** Використовуючи макет картки, студенти мають чітко показати, які дані можна називати (номер картки), а які — суворе табу (CVV-код, термін дії, ПІН-код).
- **Демонстрація «Смартфон-фортеця»:** Практичне налаштування біометричного захисту та приховування тексту сповіщень на екрані блокування безпосередньо в аудиторії.

VI. Підсумки та Q&A сесія (15 хвилин)

- **Золоте правило:** можна повідомляти лише 16-значний номер картки; ПІН-код та CVV-код (3 цифри на звороті) — суворе табу.
- **Ресурси для самоосвіти:** огляд сайту НБУ «Шахрай Гудбай» та знайомство з персонажами #Кіберпес і #КіберКіт.
- **Хто допомагає:** роль Кіберполіції у боротьбі зі злочинністю.

Для того щоб закріпити знання, отримані під час лекції від фахівців **UKRSIBBANK**, важливо перевести теоретичні правила у площину практичних навичок. Нижче наведено методи закріплення матеріалу та варіанти домашнього завдання для студентів.

Домашнє завдання

1. Творчий проєкт «Цифрова броня»

Створіть власний «рецепт» надійного пароля, використовуючи рядки з української пісні або вірша.

- **Вимога:** Пароль має містити великі/малі літери, цифри та спецсимволи (наприклад, !, @, #).
- **Завдання:** Запишіть не сам пароль, а лише логіку його створення (наприклад: «Перші літери кожного слова другого рядка пісні "Червона рута" + рік народження автора + знак оклику»).

2. Інструктаж для близьких

Проведіть коротку бесіду з батьками або дідусем/бабусею про правила платіжної безпеки.

- **Завдання:** Поясніть їм, чому не можна переходити за посиланнями «Це ти на відео?» та що робити, якщо телефонують нібито з «банку». Складіть для них «пам’ятку безпеки» на основі матеріалів лекції.

3. Дослідження ресурсів НБУ

Перейдіть на сайт за QR-кодом з презентації (проєкт #ШахрайГудбай).

- **Завдання:** Пройдіть онлайн-тест на сайті та випишіть одну нову пораду від #Кіберпса або #КіберКота, про яку не згадувалося під час лекції.

Головна порада: Ніколи не дійте емоційно. Отримали дивне повідомлення? Спочатку думайте — потім клікайте!