Сумська обласна державна адміністрація
ДЕПАРТАМЕНТ ОСВІТИ І НАУКИ
вул. Прокоф'єва, 38, м. Суми, 40016, тел./факс (0542) 36 10 97, тел. 63 51 00
E-mail: osvita@sm.gov.ua Web: www.osvita.sm.gov.ua Код ЄДРПОУ 39399524

06.09.2023 № 04.1-13/3949 На № _____ від _____

Керівникам органів управління освітою

Директорам закладів інституційного догляду та виховання дітей

Керівникам закладів позашкільної освіти

Про протидію онлайн-шахрайствам

З метою протидії та попередження вчинення онлайн-шахрайств шляхом підвищення рівня обізнаності населення про шахрайські схеми просимо забезпечити розміщення на офіційних сайтах і сторінках соцмереж закладів, установ освіти інформації, наданої відділом протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України (додається).

Про результати проведеної роботи повідомити Департамент освіти і науки Сумської обласної державної адміністрації до 15.09.2023 за наданою формою.

Додаток: на 3 арк. в 1 прим.

Директор **Вікторія ГРОБОВА**

Тетяна Бердник 36 02 90

КІБЕР ПОЛІЦІЯ
НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

П'ять речей, які ти можеш зробити, щоб захистити себе від шахраїв:

1. Будь пильним та обережним;
2. Не перераховуй кошти не верифікованим особам;
3. Уникай фейкових сторінок у соціальних мережах;
4. Не розголошуй свої персональні дані;
5. Ознайомся з шахрайськими схемами тут: (і вставляєм ссилку і QR на сайт)

З вами зв'язався працівник банку?

Пам'ятай про 5 фактів

1. Реальний працівник банку не просить надсилати кошти!

Лише шахраї наполягають на оплаті грошовим переказом чи криптовалютою;

2. Працівнику банку не потрібна інформація про ваш картковий рахунок!

Ніколи не передавай інформацію про твої рахунки тому хто телефонує;

3. Не повідомляй нікому тимчасові паролі, які приходять в смс-повідомленні!

Розголошення цієї інформації призведе до втрати коштів;

4. Не переходь за посиланнями!

Не натискай на посилання, які надсилає тобі «працівник банку»

5. Не виконуй ніяких дій у банкоматах чи терміналах Співробітник банку не надає вказівок щодо проведення маніпуляцій у банкоматах чи терміналах.

6 ознак фішингового листа

1. Звернення до вас автоматично згенероване;
2. E-mail адресанта не офіційний;
3. У листі містяться прохання надати персональні дані;
4. Наявні кнопки з гіперпосиланням на фейковий сайт;
5. Додані невідомі вкладення;
6. У тексті присутні граматичні помилки.

НЕ СТАНЬ ЖЕРТВОЮ

1. Захисти. Завжди захищайте свою особистість. Ніколи не повідомляйте свою особисту інформацію.

2. Відмов. Довіряйте своїм інстинктам. Якщо ви отримали підозрілий електронний лист, видаліть його. Якщо ви сумніваєтеся в правомірності телефонного дзвінка від незнайомця, покладіть трубку.

3. Повідом. Повідомляючи про шахрайство, ви надаєте правоохоронним органам інформацію, необхідну для припинення злочинної діяльності шахраїв і запобігання щоб інші не стали жертвами. ФІШИНГ Фішинг - (комбінація голосу та SMS) – це атака соціальної інженерії, ключовою задачею якої обманом змусити жертв надати конфіденційну інформацію по телефону.

1. Будьте пильними при отриманні дзвінків з невідомих вам номерів
2. Не передавайте дані ваших карткових рахунків чи паролю до онлайн банкінгу. Банківські працівники ніколи не запитують таку інформацію.
3. Не довіряйте особі яка телефонує, тільки тому, що вона знає про вас персональну інформацію. Шахраї можуть знайти її в Інтернеті.
4. Не перераховуйте кошти за проханням особи, яка телефонує, працівники банку ніколи не попросять вас про це.

Злочинці, які отримують гроші незаконним шляхом, повинні приховувати або відмивати джерело походження своїх коштів. Вони залучають людей для переказу грошей - дропів! Не беріть участь у вчиненні злочину, не погоджуйтесь отримувати на свої карткові рахунки чи криптогаманці кошти невідомого походження!

Тези для публікації:

ЯК НЕ ВТРАТИТИ ГРОШІ?
ПОРАДИ НА САЙТІ!
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

ШАХРАЇ ПОЛЮЮТЬ ЗА ГРОШИМА!
ЯК НЕ СТАТИ МІШЕННЮ?
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

ЗНАЙШОВ ТОВАР ЗА ПІВЦІНИ?
ТЕБЕ ЗНАЙШЛИ ШАХРАЇ!
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

ЗНАЙОМИЙ ПРОСИТЬ В БОРГ?
НАПИШИ ЙОМУ…
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

ТЕЛЕФОНУЄ ПРЕДСТАВНИК БАНКУ?
ЯК ЙОГО ПЕРЕВІРИТИ?
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

РОДИЧ ПОТРАПИВ У БІДУ?
ШАХРАЇ ЧЕКАЮТЬ І ТЕБЕ!
і qr-code з посиланням на сайт https://mriya.social/projects/stopfraud/

ВПК в Сумській області