НДІ вивчення проблем злочинності імені академіка В. В. Сташиса
bona fides

Як уберегтися в інформаційному просторі в умовах воєнного стану?

Де найбільше поширені загрози?

- Інтернет

- соціальні мережі, месенджери (Telegram, Viber, Facebook, Instagram та ін.)

- sms-розсилки та ін.

ОБЕРЕЖНО!

Шахраї використовують:

- ***псевдоблагодійність***;

- ***попит на оренду житла***. Надаються пропозиції щодо оренди фейкового житла для переселенців (або реального житла без надання послуги оренди, оскільки «орендодавець» зникає одразу ж після отримання завдатку або першого платежу за оренду);

- ***пасажирські перевезення та евакуацію***, за які Ви сплачуєте кошти наперед, а по факту вони не здійснюються;

- ***попит на товари першої необхідності***. Здійснюється «продаж» неіснуючих товарів (особливо тих, які потребують ЗСУ: військової амуніції, технічних пристроїв, продуктів харчування і т.п.);

- ***бажання виїхати за кордон*** – мають на увазі шахрайства, пов'язані з перевезенням через державний кордон України чоловіків призовного віку та тих, хто може підпадати під мобілізацію;

- ***пошук інформації про безвісно відсутніх осіб та їх викуп із полону*** – шахрайства під приводом надання інформації щодо безвісно зниклих громадян, можливостей викупу їх з полону та ін.;

- ***попит на фінансову підтримку або послуги державних органів***. Наприклад, шахраї можуть пропонувати перерахувати гроші на послуги нотаріуса або сплатити комісію для отримання державних виплат.

Як це виглядає?

◆ **фейки** (неправдива інформація про будь-кого чи будь-що, дезінформація):

- елемент інформаційної війни (*фейкові новини*);

- *інструмент шахрайства*. Треба **остерігатися**:
  1) фейкових *веб-сайтів* (такий сайт може маскуватися як під офіційні сайти державних органів та установ, так і під сайти благодійних фондів, гуманітарних центрів і т.п.);
  2) фейкових *сторінок* у соціальних мережах як організацій і установ, так і окремих волонтерів, у тому числі й реальних;
  3) фейкових *каналів* у месенджерах (Telegram, Viber та ін.)

ЯК ВІДРІЗНИТИ:

- як правило, головною відміною фейкових сайтів від реальних є їх доменне ім'я: оригінальний сайт має на кінці .ua, .com чи .gov, а фейковий – .org, .site і складається зі слів, які важко розібрати;

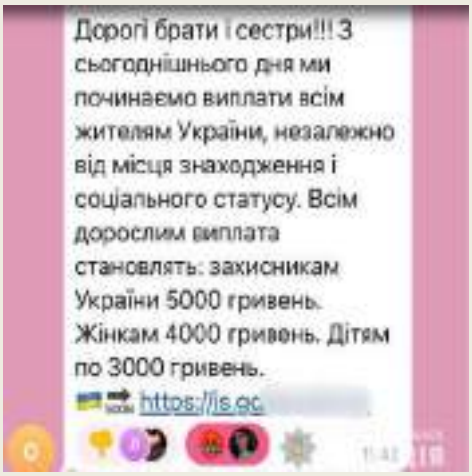
- фейкові сторінки чи акаунти, як правило, відрізняються від оригінальних однією чи кількома літерами. Тому необхідно ретельно вчитуватися у назву організації чи установи, пильно перевіряти логотип (наприклад, поширеним є розсилка спаму від імені відомих мереж магазинів «АТБ» чи «EVA»), звертати увагу на давність створення акаунту та його змістовне наповнення.

◆ **фішинг** (шахрайство, що здійснюється з метою отримання персональних даних осіб). Однією із найпоширеніших схем фішингу є пропозиція отримання грошової допомоги, замаскована під грошову допомогу від держави Україна, Організації Об'єднаних Націй, благодійних фондів і т.п. для певних категорій осіб.

Приклади:

SMS-повідомлення про грошову допомогу із текстом
«Vam narahovano Groshova dopomoga PB24 6500. Zarahuvatu…»
і далі йде посилання

⚠️Нова виплата від держави⚠️
Починаючи з 24 травня
Усі українці, що залишилися в Україні, можуть отримати виплату в розмірі 1800 грн від держави.
Ця виплата буде надходити на картку ПриватБанку кожного місяця до 1 вересня.
Оформити:
https://bit.ly/3GjxwuM



ЯК ВІДРІЗНИТИ:

- ✓ уважно вчитуватися в текст оголошення, оскільки у фейкових оголошеннях нерідко наявні граматичні помилки;
- ✓ шахраї створюють обов'язкові повідомлення-сателіти, як-то позитивні відгуки вдячності від тих, хто вже «отримав» таку допомогу (і, знову ж таки, часто у таких коментарях наявні граматичні помилки);
- ✓ як правило, текст оголошення максимально наближений до свого реального двійника, однак із певними відмінностями;
- ✓ однакові або однотипні повідомлення поширюються у різних месенджерах.

КОРИСНІ ПОРАДИ:

не переходьте за посиланнями, що надходять через sms-повідомлення або месенджери чи у електронних листах із невідомих Вам адрес скриньок

користуйтесь тільки офіційним додатком «Дія» та офіційними додатками банківських установ, які дозволяють отримати виплати на картки, емітовані ними

у жодному разі не вводьте на сторонніх ресурсах персональні або банківські дані!

перераховувати гроші тільки на рахунки офіційних благодійних фондів, рахунки, вказані на сайті НБУ, або через додаток «Дія». Якщо ви замовляли послугу отримання одноразової грошової допомоги у розмірі 6500 грн через застосунок «Дія», очікуйте сповіщення про нарахування грошей у застосунку того банку, клієнтом якого ви є. Сповіщення про нарахування грошей не містить жодних посилань, а лише текстову інформацію. Кошти автоматично будуть зараховані на ваш банківський рахунок

перевірити організацію чи фонд можна за кодом ЄДРПОУ, переглянувши сторінки організації чи її керівника в соцмережах, чи з'ясувавши, як саме оприлюднює організація / волонтер звіти про свою діяльність і витрачені кошти. Також можна звернутися до збирача коштів напряму (зателефонувавши, написавши повідомлення та ін.)

купуйте квитки на потяги чи автобуси лише на офіційних онлайн-ресурсах. У разі перевезень приватними авто незнайомими особами наполягайте на оплаті готівкою чи на картку

якщо бажаєте допомогти комусь фінансово, не переходьте за посиланням, краще введіть у пошуковій системі назву необхідного сайту і лише тоді переходьте на веб-ресурс

ЯК ЗБЕРЕГТИ СВОЇ ПЕРСОНАЛЬНІ ДАНІ:

✓ створюйте надійні, складні паролі та не використовуйте однаковий пароль для кількох ресурсів. Пароль має містити не менше 8 символів, літери, цифри та спеціальні символи, а також не містити персональних даних. За можливості, оновіть паролі до облікових записів та змініть паролі на електронних поштових скриньках;

✓ вмикайте двофакторну аутентифікацію всюди, де є така можливість. Тоді для входу до акаунту, крім логіну та паролю, потрібно ввести код підтвердження, що приходить на телефон, електронну скриньку або у відповідний додаток;

✓ не переходьте за сумнівними гіперпосиланнями, навіть якщо вони надійшли у листі від друга. Пам'ятайте, що хакери могли зламати його акаунти і розсилати з них посилання, за якими ховається вірус або фішинговий ресурс. У більшості випадків інфіковані листи надходять електронною поштою;

✓ перевіряйте правильність URL-адреси необхідного сайту. Будь-які неточності можуть означати, що ви потрапили на фішинговий ресурс;

✓ не вводьте будь-які конфіденційні дані на незнайомих сайтах та не повідомляйте такі дані стороннім;

✓ створюйте резервні копії. Це врятує від втрати важливої інформації;

✓ завантажуйте програми та додатки лише з офіційних джерел;

✓ вчасно встановлюйте оновлення операційної системи;

✓ за можливості рекомендуємо зберігати важливі дані на зашифрованих або зовнішніх носіях.

Джерела: https://cyberpolice.gov.ua/article/ataka-na-informaczijnomu-fronti---porady-kiberpolicziyi-shhodo-zaxystu-gadzhetiv-vid-vytoku-danyx-8131/; https://lb.ua/society/2022/04/13/513189_shahraystvo_period_dii_voiennogo.html

ЩО РОБИТИ, ЯКЩО ВИ ВИЯВИЛИ ШАХРАЯ:

Громадяни, які стали жертвами шахрайства, можуть повідомити про це за номером 102 або на електронну скриньку Сервісної служби кіберполіції: callcenter@cyberpolice.gov.ua.
Якщо Ви виявили шахрая у чаті, телеграм-каналі або в соціальній мережі – зверніться до адміністратора.