МІНІСТЕРСТВО У СПРАВАХ ВЕТЕРАНІВ УКРАЇНИ НАДАЄ РОЗ'ЯСНЕННЯ, ЯК НЕ СТАТИ ЖЕРТВОЮ ШАХРАЇВ В ІНТЕРНЕТІ ТА ЩО РОБИТИ, ЯКЩО ВИ ПОТРАПИЛИ У ПАСТКУ

……

Важко уявити сучасний світ без інтернету. Всесвітня павутина заполонила мало не всі сфери життя. А з 2022 року у зв'язку із введенням воєнного стану відповідно до Указу Президента від 24.02.2022 №64/2022, така online-активність призвела до зростання шахрайства в інтернеті. Використовуючи вразливий стан значної кількості людей, маніпулюючи болючими для кожного питаннями, майже одразу знайшлися й ті, для кого воєнний стан - додаткові умови для здійснення злочинної діяльності.

Міністерство у справах ветеранів України наводить практичні рекомендації громадянам України щодо зменшення можливості стати потерпілим від кримінальних правопорушень.

Нагадаємо, що відповідно до частини першої статті 190 Кримінального кодексу України **Шахрайство** – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою. Частина третья статті 190 Кримінального кодексу України передбачає, що шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки **карається позбавленням волі на строк від трьох до восьми років.**

Сайти-двійники, що імітують діяльність державного органу України

На сьогоднішній час найпоширеним є шахрайство, що полягає у створенні сайтів-двійників. Сторінка, яку ви відвідуєте, візуально виглядає як справжня: має ту ж кольорову гаму, містить приблизно ту ж саму інформацію, що й офіційний сайт, однак у гіперпосиланні вказані зайві букви або цифри. Здійснивши ідентифікацію (автентифікацію) на сайті-двійнику вказавши власні персональні дані, ви потрапляєте у пастку шахраїв. 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, звертати увагу на давність створення акаунту та його змістовне наповнення.

Шахраї, що використовують ваші персональні дані проти вас

Ніколи не залишайте свої персональні дані на незнайомих або підозрілих сайтах. Необхідні вам товари чи послуги ви не зможете отримати, а ваші персональні дані можуть бути використані проти вас. Тому перед введенням своїх даних переконайтеся, що ви точно перебуваєте на офіційному сайті.

В період воєнного стану шахраї використовують:

- псевдоблагодійність;
- надання пропозиції (послуг) щодо забезпечення житлом, земельною ділянкою для різних категорій осіб (без надання самих послуг, оскільки "шахрай" зникає одразу ж після отримання завдатку або першого платежу за певну послугу);

- попит на товари першої необхідності (здійснюють «продаж» неіснуючих товарів, а також «надають» неіснуючі послуги особливо тих, що потребують вразливі особи);
- пошук інформації в базах даних (шахрайство під приводом надання інформації щодо витягів із баз реєстрів, або надання іншої інформації);
- попит на фінансову підтримку (шахраї пропонують перерахувати гроші на послуги нотаріуса або сплатити комісії для отримання державних виплат.

Щоб не стати жертвою оголошення, дотримуйтесь трьох легких правил:

1. Уважно вчитуйтесь в текст оголошення, оскільки у фейкових оголошеннях нерідко наявні граматичні помилки.

2. Як правило шахраї використовують текст оголошення максимально наближений до свого реального двійника, однак із певними відмінностями.

3. Звертайте увагу на повідомлення-сателіти, як-то позитивні відгуки вдячності від тих, хто вже «отримав» таку допомогу, зазвичай в них є граматичні помилки.

Щоб зберегти свої персональні дані, дотримуйтесь таких правил:

- ✓ не переходьте за сумнівними гіперпосиланнями, навіть якщо вони надійшли у листі від вашого знайомого, друга або члена родини (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;
- ✓ **у жодному разі** не вводьте на сторонніх ресурсах власні персональні або банківські дані. Не наддавайте ваші особисті персоніфіковані/реєстраційні дані постороннім особам та неперевіреним джерелам.
- ✓ нікому не повідомляти термін дії банківської карти та CVV-код;
- ✓ не користуватися неперевіреними оголошеннями щодо роботи, яка обіцяє швидко вирішити всі питання за внесення певної суми завдатку (варто пам'ятати золоте правило – «безкоштовний сир тільки у мишоловці»);
- ✓ завантажуйте файли, програми та додатки лише з офіційних джерел.

Що робити, якщо ви виявили шахрая або стали його жертвою

- ✓ 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 сайту, з метою блокування сторінки шахрая, а також зателефонуйте в банк, через який було здійснено платіжні операції, повідомте, що переказ здійснено на картку шахрая.
- ✓ Зберіть інформацію, що підтверджує факти вчинення щодо вас шахрайських дій: чеки про оплату, квитанції з банку про проведення грошових операцій, роздруківки оголошень, посилання на сайт, все що можна.
- ✓ Після притягнення винної особи до кримінальної відповідальності, ви можете звернутись до суду з вимогою відшкодування матеріальної та моральної шкоди. Згідно із **частиною першою статті 1212** Цивільного кодексу України особа, яка,

набула майно або зберегла його у себе за рахунок іншої особи (потерпілого) без достатньої правової підстави (безпідставно набуте майно), зобов`язана повернути потерпілому це майно. Особа зобов'язана повернути майно і тоді, коли підстава, на якій воно було набуте, згодом відпала.

- ✓ Дієвим способом захисту уразі, якщо ви перерахували кошти шахраям в інтернеті, може бути звернення до суду з позовом про повернення безпідставно набутих коштів до власника банківського рахунку, на який здійснено зарахування коштів.
- ✓ Для отримання правової допомоги ви можете звернутись у найближчий до вас місцевий центр з надання безоплатної вторинної правової допомоги або бюро правової допомоги, адресу і контактний телефон яких ви зможете дізнатися за номером Єдиного контакт-центру системи безоплатної правової допомоги − 0 800 213 103 (цілодобово та безкоштовно в межах України зі стаціонарних та мобільних телефонів), або за посиланням: https://www.legalaid.gov.ua/tsentry/.

Міністерство у справах ветеранів України
2023 рік