

Управління соціального захисту населення Подільської РВА інформує:

Як ветеранам та членам їхніх сімей не стати жертвою кібершахраїв

Кіберфронт для ворога не менш важливий, аніж гаряче поле битви. За допомогою всесвітньої павутини агресор намагається поширити кремлівську пропаганду, ввести українців в оману, провокує на співробітництво, шантажує і банально обкрадає. Так само у час війни активізувалися і кримінальні шахраї, які користуються різноманітними схемами облуди та неправомірної наживи за допомогою інтернет-інструментів. Зокрема, відомим став вид «воєнного шахрайства» - псевдоволонтери, які нібито збирають кошти на допомогу ЗСУ, пораненим захисникам чи їхнім родинам. А також фішинг — одна з найпоширеніших афер.

Лиходії переважно використовують фішинг-посилання у схемах з виплатами, що так чи інакше пов'язані з війною, вони створюють сторінки-клони державних та міжнародних організацій, благодійних фондів, банків, пропонують за гроші надати інформацію щодо перебування члена родини, який пропав безвісти або потрапив у полон, що виявляється фейковою. Аферисти для цього вимагають, наприклад ввести персональні дані та номер банківської картки нібито для зарахування коштів або надання певної соціальної послуги. Отримавши потрібні реквізити, вони привласнюють гроші з чужих рахунків.

Тому надзвичайно важливо, аби щонайбільше громадян дотримувалися правил кібергігієни.

Тим часом Міністерство у справах ветеранів України нагадує ветеранам та членам їхніх сімей про дотримання правил кібергігієни:

✓ не повідомляти конфіденційну інформацію, зокрема дані банківських карток, стороннім;

(Для виплати тих чи інших соціальних послуг Міністерство у справах ветеранів України використовує лише номер особистого рахунку ветерана чи члена його сім'ї (IBAN));

✓ не переходити за сумнівними гіперпосиланнями, які надсилають вам.

(Зверніть увагу, що офіційні сторінки державних органів, благодійних організацій, банківських структур у месенджерах та соціальних мережах мають бути верифікованими (містити позначку ✓));

✓ отримувати інформацію, особливо з приводу фінансових виплат від Міністерства у справах ветеранів, лише з офіційних джерел.

(Офіційно щодо надання та актуальності послуги інформацію можна отримати на сайті Мінветеранів <https://mva.gov.ua/> чи за допомогою мобільного додатку ДІЯ);

✓ у разі підозри шахрайських дій - негайно повідомляйте у правоохоронні органи.

! ПАМ'ЯТАЙТЕ, що навіть в умовах війни, справжні співробітники банку, або працівники держустанов не запитують таку інформацію.

□ Якщо ви стали жертвою кібершахрайства або виявили шахрайські дії, то можете звернутись за наданням правової допомоги чи за консультацією:

➔ Сайт кіберполіції: <https://ticket.cyberpolice.gov.ua/>, або Департамент кіберполіції, зателефонувавши за номером 0 800 505 170 або написати на електронну пошту callcenter@cyberpolice.gov.ua, також можете звернутись до найближчого відділення поліції.

➔ Отримати безоплатну правову допомогу можна і за безкоштовним номером 0 800 213 103.

➔ Ознайомитись з актуальною інформацією щодо осіб, які перебувають у розшуку, можна на сайті Служби безпеки України <https://ssu.gov.ua/u-rozshuku>

➔ Ознайомитись із актуальною інформацією щодо бази даних санкційних списків юридичних та фізичних осіб, на яких вже накладені санкції, можна на сайті НАЗК <https://sanctions.nazk.gov.ua/sanction-lists/>

□ Корисні інформаційні посилання та посилання на освітні серіали:

- Поради як діяти в екстремальних ситуаціях та як подбати про кібербезпеку від спеціалістів СБУ.

<https://ssu.gov.ua/yak-podbaty-pro-kiberbezpeku>

- Допомога в розблокуванні свого цифрового світу без платежів кібершахраїв <https://www.nomoreransom.org/uk/index.html>

• Дія. Освітній серіал “Обережно!!! Кібершахраї. Як захистити себе від шахраїв в інтернеті”. <https://osvita.dii.gov.ua/cou.../attention-cyber-fraudsters>

• Дія. Освітній серіал “Медіа грамотність. Як розпізнати брехню, маніпуляцію в інтернеті”.

<https://osvita.dii.gov.ua/.../mediagramotnist-u-casi...>

• Дія. Освітній серіал “Основи кібергігієни. Як захиститись від хакерів”.

<https://osvita.dii.gov.ua/courses/cyber-hygiene>

• Дія. Освітній серіал “Персональні дані і політика приватності. Що це та як безпечно ним управляти”. <https://osvita.dii.gov.ua/courses/personaldata>

• Дія. Освітній серіал “Смартфон для батьків. Як користуватись смартфоном: інтернетом, дзвінки, облікові записи, безпека, налаштування під себе”.

<https://osvita.dii.gov.ua/.../gostiovy-kurs-smartfon...>

• Дія. Освітній серіал “Бути поруч: Основи психологічної підтримки дітям. Як працювати з дітьми під час війни та надавати ефективну психологічну допомогу”. <https://osvita.dii.gov.ua/.../buty-poruch-kurs-z-osnov...>

МІНВЕТЕРАНІВ ІНФОРМУЄ



МІНІСТЕРСТВО
У СПРАВАХ
ВІТЕРАНІВ
УКРАЇНИ