Кібербезпека під час війни

З початком повномасштабного вторгнення росії на територію України ворог активно використовує інформаційні технології для досягнення своїх цілей. Кібербезпека під час війни надзвичайно важлива, оскільки ворог може використовувати кібератаки для проведення пропаганди та дезінформації. Ризики включають можливість впливу на громадську думку через розповсюдження фальшивих новин, маніпулювання соціальними мережами та злам медіа-ресурсів. Це може призвести до паніки серед населення, зниження морального духу та навіть до поширення розбрату та зневіри в українському суспільстві.

Правила інформаційної гігієни на цифровому фронті під час війни

Зараз у соцмережах і медіа багато фейків та дезінформації. Усе це вороги роблять для того, щоб українці втратили віру в перемогу й опустили руки.

Як розпізнати фішинг?

✅ **Перевірте URL-адресу**. Офіційні сайти маркетплейсів мають правильні та безпечні доменні імена (наприклад, "rozetka.ua" або "olx.ua"). Якщо ж у посиланні присутні сумнівні символи, додаткові цифри чи літери, або якщо адреса виглядає трохи зміненою, наприклад, "roz3tka.ua" або "olx.com.ua", це може бути ознакою фішингу.

✅ **Перевірте дизайн сайту**. Фальшиві сайти часто виглядають схоже на оригінальні, але зазвичай мають низьку якість графіки, помилки у тексті або незвичну структуру. Якщо ви помітили подібні недоліки, краще покинути сайт.

✅ **Звертайте увагу на розсилки**. Легітимні маркетплейси зазвичай не просять вводити особисту інформацію через електронну пошту або месенджери. Якщо ви отримали таку вимогу, будьте обережні.

✅ **Перевірка через офіційний сайт або додаток**. Якщо вам здається, що з вами зв’язуються з офіційного маркетплейсу, краще зайти на сайт або відкрити додаток через перевірений канал, а не за посиланням у листі чи повідомленні.

❌ **Остерігайтеся підозрілих повідомлень**. Якщо ви отримали листи або повідомлення через соцмережі з посиланнями на "подарунки" чи "знижки", це може бути спробою заманити вас на фальшивий сайт. Часто такі повідомлення містять заклики терміново ввести дані або здійснити оплату.

Як захистити себе від фішингу?

✅ **Використовуйте двофакторну автентифікацію**. Більшість сучасних маркетплейсів пропонують додаткові засоби безпеки, такі як SMS-коди або підтвердження через додаток. Це знижує ризик несанкціонованого доступу до вашого акаунту.

✅ **Перевіряйте покупку через додаток чи офіційний сайт**. Не вводьте платіжні дані на сторонніх сайтах. Завжди використовуйте лише перевірені ресурси.

✅ **Слідкуйте за оновленнями безпеки**. Переконайтеся, що ваш браузер та операційна система оновлені до останніх версій. Це допоможе захистити вас від багатьох онлайн-загроз.

✅ **Будьте обережні з публічними Wi-Fi мережами**. Уникайте здійснювати покупки чи вводити особисті дані, коли підключені до незахищених мереж.

❌**Не довіряйте занадто гарним пропозиціям**. Якщо якась пропозиція здається надто вигідною, щоб бути правдою, швидше за все, це пастка.

Тож просимо дотримуватися правил, які допоможуть вам вистояти під час інформаційної атаки окупантів:

1. Користуйтеся офіційними джерелами інформації (зібрали їх http://stopfraud.gov.ua/),а також офіційними сторінками держслужбовців та органів місцевого самоврядування.
2. У жодному разі не ведіться на рекламні дописи в соцмережах із псевдосторінок СБУ чи інших держустанов. Їх публікує ворог, щоб викликати у вас довіру. Перевіряйте офіційні сторінки установ на достовірність такої інформації.
3. У жодному разі не поширюйте інформацію про переміщення українських військ, так ви здаєте позиції ворогу!
4. Поширюйте правду про війну, яку веде рф в Україні, у своїх соцмережах. Пам'ятайте: вони теж є інформаційною зброєю проти ворога!
5. Робіть дописи для своєї аудиторії в соцмережах, спілкуйтеся зі знайомими адміністраторами груп і каналів в інших країнах та поширюйте інформацію через них. Поширюйте правду до росіян, оскільки там повністю обмежений доступ до правдивої інформації.
6. Підтримуйте «гігієну своїх пристроїв»: блокуйте пристрої щоразу після закінчення роботи, встановлюйте застосунки лише з офіційних сервісів, не користуйтеся невідомим Wi-Fi.
7. Захистіть свої соцмережі: встановлюйте складні паролі, не додавайте в друзі невідомі акаунти, увімкніть двоетапну автентифікацію.
8. Підтримуйте дух нашої армії! Пишіть слова подяки, підбадьорюйте українців!
9. Долучайтеся до проєкту "BRAMA" https://t.me/brama_channel та протидійте пропаганді ворога разом із тисячами українців.

Як розпізнати спробу вербування?

– Вас просять передавати інформацію, фотографувати об’єкти чи відстежувати пересування військових.

– Обіцяють хороший заробіток без зусиль.

– Переконують, що “ніхто не дізнається” і що “нічого страшного тут немає”.

– Чинять тиск, маніпулюють, шантажують або навіть залякують.

Що робити, якщо хтось намагається вас завербувати?

- Не передавайте жодної інформації, навіть якщо вона здається неважливою.
- Негайно розкажіть батькам, вчителям або зверніться до поліції.
- Пам’ятайте: незнайомець у мережі може бути зовсім не тим, за кого себе видає. Не дозволяйте нікому втягнути вас у гру, правила якої пише злочинець. Залишайтеся обережними, бережіть себе та своїх друзів!