Як уникати шахрайства в Інтернеті?

*Корисні поради сформовані на основі освітніх серіалів з питань безпечного поводження у мережі Інтернет (*Дія. Цифрова освіта https://osvita.diia.gov.ua/ *)*

Ми живемо в бурхливий час розвитку технологій, користуємось різними сучасними пристроями. Звичайно, це полегшує нам життя та урізноманітнює його. На жаль, прикрощі та небезпеки також можуть траплятися. Що потрібно знати, щоб уникати шахрайства в Інтернеті? Які бувають шахрайства?

1. **Складні паролі**. Хакери давно створили словники для підбору паролів. Вони можуть паролі зламувати та викладати у відкритий доступ. Отже, потрібно використовувати різні складні паролі та їх періодично змінювати. Також можна використовувати двоетапну перевірку. Корисно встановити пароль для доступу до екрану смартфону, а також до інформації.
2. **Оновлення програмного забезпечення.** Якщо ми не оновлюємо програми своєчасно, зловмисники можуть скористатися вразливостями під час атак, в тому числі і у цілях шахрайства. Хакер після кібератаки може заволодіти персональними даними. Крім того, пристрої після оновлення краще працюють, покращуються їх функції. Отже, оновлювати потрібно всі пристрої, підключені до Інтернету та їхні операційні системи. Важливо користуватись антивірусними програмами (регулярно їх оновлювати), які виявляють та знешкоджують комп'ютерні віруси.
3. **Резервне копіювання даних (бекап).** Процес створення копії даних на цифровому носії для подальшого відтворення цих даних в оригінальному місці їх розташування в разі пошкодження або руйнування. Це фактично копіювання важливих файлів на іншому носії або диску. Для зберігання резервних копій підходять також хмарні сервіси. Частота створення резервних копій залежить від частоти зміни файлів, які ви резервуєте. Отже, для хмарних сервісів потрібно використовувати складні паролі та, де можливо, підключати двофакторну (двоетапну) автентифікацію (перевірку). Зовнішні носії потрібно шифрувати або шифрувати файли, які ви зберігаєте.
4. **Фішинг, смішинг, вішинг, бейтінг .**
   Фішинг – виловлювання персональних даних довірливих користувачів. Зловмисники можуть заразити комп'ютер чи смартфон вірусом, потім вимагати гроші за «лікування» пристрою, використати інтернет – банкінг та знімати гроші з банківських карток, дані облікового запису. Шахраї намагатимуться через листи чи SMS спонукати вас перейти на фішинговий сайт через кнопку або посилання для підтвердження реєстрації тощо. Важливо перевіряти справжність сайту, його домен та

захищеність (оформлення адресного рядка, протокол шифрування даних https на початку адреси). Жодним чином не можна вводити логін та пароль на сумнівних сайтах та не переходити за посиланнями. Не відкривайте будь – які посилання від незнайомців. Уважно переглядайте електронні листи та не переходьте за посиланнями, не завантажуйте файли, не розпаковуйте архіви. Уважно перевіряйте адресу відправника та саме посилання. Користуйтеся антивірусом. Нікому не надавайте свої паролі та логіни, змінюйте паролі. **Смішинг** – надсилання шахраями повідомлень із цікавими пропозиціями або попередженнями, з якими можна ознайомитись, перейшовши за посиланням або перетелефонувавши. **Вішинг** - телефонне шахрайство, метою якого є отримання реквізитів банківських карток або будь – якої іншої конфіденційної інформації. Шахраї повідомляють, що виправити ситуацію можна лише негайними діями. Важливо не панікувати. Потрібно передзвонити на номер і розпитати про обставини та навіщо потрібні гроші. Зазвичай шахраї не вдаються в деталі, одразу кидають слухавку. Справжні банківські співробітники ніколи не запитують персональні дані клієнтів. В жодному разі не можна повідомляти CVV – код із зворотньої сторони банківської картки, PIN – код. Ніколи не повідомляйте незнайомцям коди з ваших SMS. Не переказуйте гроші на чужий рахунок під виглядом збереження коштів – це шахрайство. Перевіряйте інформацію щодо небезпеки життю чи стану близьких людей. **Бейтінг** – спосіб шахрайства, коли підкидають флешки або інші USB – носії з вірусами. Іноді це дає можливість прослуховувати людину або визначати її місце знаходження. Знайдені флешки краще викинути, а подаровані - можна перевірити та відформатувати (якщо є якісь файли, то вони будуть знищені).

5. **Як безпечно проводити платежі в Інтернеті.** Купувати в Інтернеті не завжди безпечно адже мета деяких фейкових магазинів виманювати персональні дані для крадіжки грошей з карток. Не потрібно розголошувати номер банківської карти, строк її дії, CVV – код, фінансовий номер, який прив’язаний до картки, надавати перевагу післяоплаті. Не використовуйте фінансовий номер для реклами чи оголошення. Можна використовувати окрему картку для покупок в Інтернеті, але стан її рахунку також треба перевіряти через онлайн – банкінг.
6. **Якщо телефон загублено чи вкрадено…** Важливою деталлю смартфона є його сім – карта, до неї часто прив’язаний онлайн – банкінг, приватне листування, фото, фото документів, доступ до соціальних мереж. Встановлюйте пароль для використання сім – карти, налаштовуйте додаткові паролі для входу в застосунки, не зберігайте паролі входу на

телефоні, налаштуйте функцію пошуку втраченого пристрою, використовуйте хмарні середовища та робіть резервне копіювання інформації. Можна також звернутися до мобільного оператора та заблокувати сім – карту. Пошук телефона можна здійснювати за IMEI – серійний номер пристрою, що встановлюється виробником та є унікальним. За цим номером з'являється можливість встановити номери сімок, якими користувався власник.

Викравши телефон, шахраї можуть використовувати аудіоповідомлення у соцмережах та маседжерах, а потім телефонувати голосом ваших знайомих та рідних.

Висновок: дотримуйтесь правил кібер – гігієни та будьте пильними, адже шахраї винахідливі.

Корисні інформаційні ресурси та можливості, які можна використовувати з питань кіберзахисту та кібергігієни:

https://disted.edu.vn.ua/media/bp/html/oppilaille.htm

https://digitaledu.org.ua/

https://cyber.volunteer.kiev.ua/#/

Освітні серіали на платформі «Дія. Цифрова освіта»:

https://osvita.diia.gov.ua/courses/cybernanny

https://osvita.diia.gov.ua/courses/in-safety

https://osvita.diia.gov.ua/courses/cyber-hygiene

https://osvita.diia.gov.ua/courses/cyberbullying