Основи інформаційної безпеки

Безпека в Інтернеті.
Безпечне зберігання даних.

Загрози під час роботи в Інтернеті

Серед основних загроз використання комп'ютерних мереж для користувачів, виділяють:

- Комунікаційні ризики
- Контентні ризики
- Споживчі ризики
- Технічні ризики

Комунікаційні ризики

- ризики, що пов’язані зі спілкуванням у мережі та використанням онлайн-ігор:

БУЛІНГ - залякування, приниження, цькування, переслідування, компрометація людей з використанням особистих або підробних матеріалів, розміщених в Інтернеті, надсилання повідомлень з використанням різних сервісів;

КОМПРОМЕТУВАТИ – виставляти в негарному вигляді, шкодити добрій славі;

КІБЕР – ГРУМІНГ - входження в довіру людини для використання її в сексуальних цілях;

ОНЛАЙН – ІГРИ – надмірне захоплення може призвести до втрати реальності, нерозуміння та несприйняття норм і правил людського співіснування, комп’ютерної залежності.

Контентні ризики

- ризики, що пов’язані з доступом до матеріалів, розміщених у мережі, матеріалів шкідливого характеру або таких, що не відповідають віковим особливостям розвитку дитячої психіки.

Такі матеріали як правило містять:

- ✓ сцени насилля, жорсткої поведінки з людьми та тваринами;
- ✓ пропаганду расової або національної ненависті;
- ✓ рекламу або пропаганду використання тютюну, алкоголю та наркотиків, азартних ігор;
- ✓ пропаганду релігійних вірувань, заборонених законодавством, або спільнот, що не мають офіційних дозволів на свою діяльність;
- ✓ пропаганду шкідливих лікарських засобів і методів боротьби з хворобами, відмови від лікування;
- ✓ нецензурну лексику;
- ✓ матеріали для дорослих.

Споживчі ризики - **ризики, що пов’язані з порушенням прав споживачів:**

- ✓ реклама та продаж через мережу інтернет-магазинів низькоякісної продукції;
- ✓ купівля підроблених товарів відомих виробників;
- ✓ втрата коштів через невиконання обіцянок надіслати товар, невідповідність товару за якістю або за виробником (шахрайство);
- ✓ викрадання персональних даних для зняття коштів без відома користувача з його рахунків.

Технічні ризики - ризики, що пов’язані з роботою шкідливих програм:

- ✓ Віруси
- ✓ Хробаки (черв’яки)
- ✓ Трояни, даундлоадери
- ✓ Скрипт-віруси
- ✓ Дропери
- ✓ Боти
- ✓ Скімінг
- ✓ Руткіти
- ✓ Експлойти
- ✓ Бекдори
- ✓ Шпигунські програми
- ✓ Рекламні модулі або Adware
- ✓ Діалери

Загрозу також становить фішинг та спам як різновид інтернет-шахрайства.

Шляхи захисту даних

Серед заходів безпеки, яких повинен дотримуватися кожен користувач, перше місце займає його особиста організованість і відповідальне ставлення до зберігання важливих даних.

Розрізняють три шляхи захисту даних:

- Захист доступу до комп'ютера
- Захист даних на дисках
- Захист даних в Інтернеті

І пам'ятайте!!

- ***Двохфакторна авторизація*** - це спосіб входу до акаунту, при якому потрібно **крім введення логіну та паролю** виконати певну додаткову дію, наприклад **ввести код**, отриманий:
- в смс
- на електронну пошту
- в голосовому повідомлення
- Також, для дуже важливих акаунтів використовуються:
- унікальні зовнішні накопичувачі
- зчитувачі біометричних даних

Трохи гри)

Тисни

Відповідь

Ю	З	Т	І	Я	М	К	Ь	Е	З	Є	Е	П
Щ	Ї	Ї	С	Л	А	Н	П	П	Є	Г	О	А
Ґ	А	Щ	Е	М	Ф	Й	С	Ж	Й	Ї	О	Р
Г	Д	Ч	Т	К	О	З	Є	Ґ	П	Н	У	О
И	Т	Н	Б	Е	З	П	Е	К	А	Ю	Л	Л
Ж	У	Д	Г	Ш	М	П	Р	О	Ф	І	Л	Ь
Є	Л	І	Ї	Л	Ї	Б	З	М	Ж	Г	У	Ч
П	О	В	І	Д	О	М	Л	Е	Н	Н	Я	В
Н	Г	Ґ	В	А	К	А	У	Н	Т	Ш	Й	Т
Ї	І	Н	Т	Е	Р	Н	Е	Т	Л	Ї	Ч	Ч
І	Н	Р	Е	Є	С	Т	Р	А	Ц	І	Я	Щ
Т	Ь	Ь	Й	Ж	У	М	Е	Р	Е	Ж	А	Г

1. **БЕЗПЕКА**
2. **МЕРЕЖА**
3. **РЕЄСТРАЦІЯ**
4. **ПОВІДОМЛЕННЯ**
5. **ПРОФІЛЬ**
6. **АКАУНТ**
7. **ПАРОЛЬ**
8. **КОМЕНТАР**
9. **ІНТЕРНЕТ**
10. **ЛОГІН**