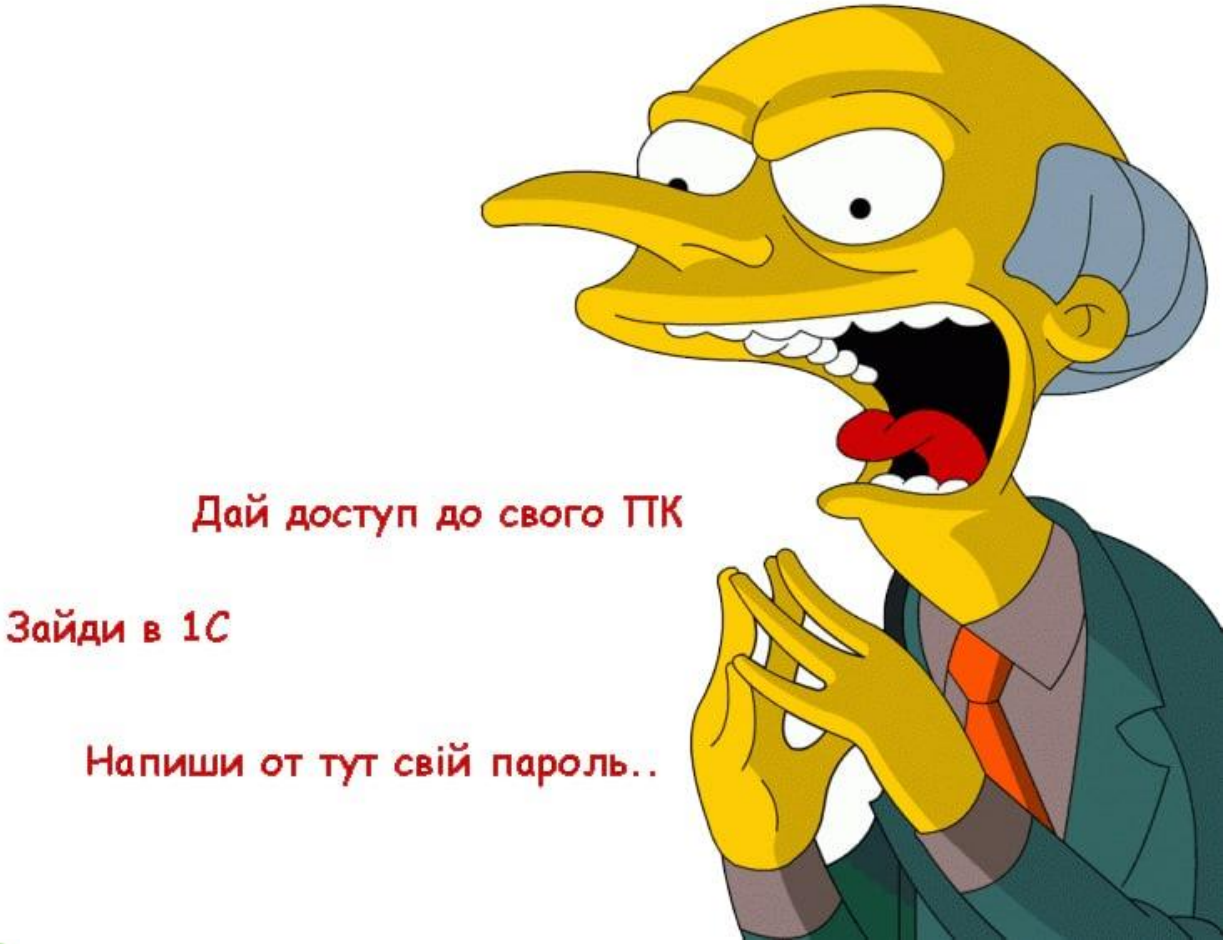

- Привіт, це з ІТ відділу. Потрібно дещо перевірити. Даси доступ через Team Viewer ?
- Так, звичайно. Глянь, в мене ще тут комп'ютер підвисає..
- Без проблем! А покажи чи ти правильно в 1С заходиш. А в пошту?
- …
- Я тут скопіюю ці файли, їх треба перевірити на віруси.
  А взагалі залиш свій пароль щоб я тебе не відволікав, можеш поки піти попити кави.

Думаєш ти б не купився? Звучить переконливо..
Описана ситуація досить типова в період віддаленої роботи, адже існує потреба віддаленого вирішення технічних питань.
Зловмисник це знає, тому якщо в нього не вдалось зламати твій складний пароль, він спробує виманити його методами Соціальної інженерії.

Не соромся:
- Якщо працівник тех-підтримки не представився, уточни його дані.
- Поцікався з якого приводу дзвінок. Особливо якщо ти попередньо не залишав звернень!
- Перевір чи знає він кому телефонує, адже він міг отримати базу номерів без імен.
- Якщо діалог викликає підозри, звернись по номеру 0(67)-678-95-38 в ІТ відділ та переконайся у необхідності виконання робіт.

Соціальна інженерія - це не тільки прямий контакт з зловмисником.

Це ті ж Фішингові листи, про які ти неодноразово чув.
Це блискуча флешка на парковці чи поблизу офісу, яка будить в тобі бажання встромити її у свій ПК.
Ніколи не приєднуй до ПК носії невідомого походження, хакери часто розкидають такі

«подарунки» поблизу компаній чи в людних місцях. Це вірний спосіб надати сторонній особі доступ до частини конфіденційних даних, а то і до управління всім ПК.

Багато зловмисників можуть претендувати на диплом з психології і старатимуться обійти твою пильність найекстравагантнішими методами.
Не приймай поспішних рішень, користуйся лише перевіреними ресурсами і тримай свої облікові дані в секреті.

Безпечного тобі дня! Зустрінемось в «Інформаційній безпеці».