Правила безпеки використання хмарних сховищ

#КібербезпекаФінансів

Хмарні сховища – це зручний сервіс для зберігання та обробки будь-якої вашої особистої інформації, що тісно інтегровані в настільні ПК і мобільні операційні системи на смартфонах. Завдяки ним ви можете володіти доступом до усіх ваших даних з будь-якої точки планети та з будь-якого доступного вам пристрою. Це надзвичайно крута перевага, однак це також відкриває великі можливості для тих, хто так само може отримати ваші файли — для кіберзлочинців. **Ось декілька правил щодо забезпечення безпеки користування хмарними технологіями:**

1. **використовуйте надійні паролі та двофакторну автентифікацію.** Що це і як працює – читайте на **#КібербезпекаФінансів;**
2. **здійснюйте регулярний аудит і перевірку ваших файлів та загальних папок,** які ви зберігаєте у вашому хмарному сховищі. Також постійно переглядайте, з яких саме пристроїв є доступ до вашого хмарного сховища;
3. **обов'язково видаляйте кеш "вже видалених файлів".** Багато хмарних сервісів зберігання використовують так звану "корзину", зберігаючи протягом певного часу видалені вами файли на випадок, якщо ви раптом захочете їх відновити. Часто ця функція є дуже корисною і може стати перевагою в разі відновлення випадково видаленої інформації. Однак необхідно впевнитися, що важливі конфіденційні файли будуть цілком знищені та ніхто більше не зможе їх відновити. Тому слід перевіряти "корзину" з видаленими файлами всередині хмарних сховищ, якщо там зберігаються важливі конфіденційні файли;
4. **увімкніть сповіщення та повідомлення про дії в акаунті.** Це можна зробити в налаштуваннях вашого акаунту. Завдяки цій функції ви дізнаєтеся, якщо хтось сторонній увійшов до вашого акаунту;
5. **деактивуйте доступ до хмарних сховищ для пристоїв, які ви вже давно не використовуєте;**
6. **увімкніть параметри відновлення облікового запису.**

Національний банк України

Державна служба спеціального зв'язку та захисту інформації України