ЯК ПРИДУМАТИ НАДІЙНИЙ ПАРОЛЬ

Одне з найгостріших питань сучасного світу — кібербезпека. Оскільки кожен з нас користується соціальними мережами, електронною поштою, месенджерами та різними онлайн-сервісами, важливо знати, як надійно захистити свої дані. А для власників сайтів, інтернет-магазинів, блогів захищений доступ до облікових записів — невіддільна складова успішного існування бізнесу.

Головним помічником у боротьбі за кібербезпеку є складний для хакерів пароль. Ділимося з вами, як створити надійний пароль, де і як правильно його зберігати та яких заходів треба вживати для того, щоб він забезпечував стабільний захист від зловмисників.

Чому важливо правильно зберігати паролі

Користування паролями — важлива складова роботи з будь-яким програмним забезпеченням або ресурсами. При цьому паролі є невіддільною частиною інформаційної безпеки компанії. Вони забезпечують захист облікових записів користувачів, користувацьких даних та доступу до них. Використання слабкого пароля може призвести до того, що сторонні особи отримають доступ до даних. Також це може порушити працездатність інформаційних систем інших компаній (наприклад, постачальника послуг хостингу).

Тож співробітники компанії, постачальники, підрядники або відвідувачі — усі користувачі, що мають доступ до інформаційних систем компанії, несуть відповідальність за безпечне створення паролів та їх захист.

Що таке слабкий та стійкий паролі

Кожен з нас використовує паролі для багатьох цілей. Найбільш поширені з них — вхід у комп'ютер, електронна пошта, авторизація на різних веб-ресурсах тощо. Лише за рідкісним винятком зустрічаються системи з одноразовими паролями. Переважно ми використовуємо паролі багаторазово, тож кожен користувач має знати вимоги до створення надійних паролів.

Розглянемо детальніше, яким має бути безпечний пароль та яких комбінацій слід уникати.

Ознаки слабкого пароля:

- містить менше ніж 12 символів;
- слово зі словника;
- слово, що використовується у повсякденному житті, наприклад, імена або прізвища друзів, колег, акторів або казкових персонажів, клички тварин;
- комп'ютерний термін, команда, найменування сайту, апаратного або програмного забезпечення;
- варіації найменування компанії або торгової марки;
- день народження або інша персональна інформація, наприклад, адреса, номер телефону тощо;
- регулярні послідовності символів і цифр, наприклад, 111111, abcde, qwerty тощо;
- що-небудь з перерахованого вище у зворотному написанні;
- що-небудь з перерахованого вище із додаванням цифри на початку або в кінці.

Наприклад, серед найбільш поширених паролів по всьому світу вже багато років залишаються такі комбінації та слова: 123456, 123456789, 123123, 123321, 111111, password, qwerty, qwerty123, iloveyou, princess, admin. Часто у паролях трапляються також назви солодощів або марок автомобілів, наприклад, cocacola, snickers, mercedes, ferrari. Лідують і герої з кіно- та мультфільмів, зокрема superman та spiderman, а також назви популярних світових гуртів (наприклад, metallica). У 2019 році тенденція, на жаль, залишається незмінною. Перелік лише поповнився не менш уживаними слова, як-от, football, monkey, donald, charlie.

Тепер розглянемо, з яких елементів має складатися надійний пароль.

Характерні риси стійкого пароля:

- містить великі та малі літери;
- містить цифри та символи;
- понад 8 символів довжиною;
- не є словом ні на одній з мов, діалектів, жаргонів, сленгу;
- не ґрунтується на персональній інформації.

А ще безпечний пароль не має зберігатися в паперовій або електронній формі без відповідного захисту носія.

Як створити пароль, що легко запам’ятовується

Пароль має бути не лише стійким, але й добре запам'ятовуватися. Тож як скласти таку влучну комбінацію? Ми пропонуємо створити пароль на основі назви пісні, фрази або асоціації з ними. Наприклад, ваша улюблена пісня — The Beatles - Let It Be (1970). Тоді пароль може виглядати так: **TB-19lib70**.

Які паролі не можна використовувати

Для облікових записів користувачів компанії не можна використовувати:

- той самий пароль, що й для інших інформаційних систем (наприклад, домашній інтернет-провайдер, безкоштовна електронна пошта, форуми тощо);
- один і той же пароль для різних корпоративних систем;
- однакові паролі в операційних системах Unix і Windows.

Чого слід уникати у роботі з паролями

1. Повідомляти пароль інших особам, зокрема адміністративному персоналу.
2. Повідомляти принципи створення пароля (наприклад, на основі прізвища).
3. Повідомляти пароль в електронних опитуваннях, незнайомих формах авторизації або де-небудь ще.

4. Передавати пароль колегам на час вашої відсутності, відпустки або відрядження.

Додаткові заходи для захисту ваших даних

Подбайте про те, щоб на комп'ютері була ввімкнена заставка, захищена паролем, яка активуватиметься через 10 хвилин вашої бездіяльності. При цьому вхід в систему не повинен виконуватися автоматично.

Крім того, блокуйте комп’ютер кожного разу, коли залишаєте робоче місце. Заблокувати ПК можна кількома способами. Для ОС сімейства Windows діє така послідовність: натискаємо сполучення клавіш **Windows + L** або **Ctrl-Alt-Delete** та обираємо відповідне значення в доступному списку операцій. Якщо треба заблокувати ПК з ОС сімейства Linux, використовуємо сполучення клавіш **Ctrl + Alt + L.**

І ще декілька правил, які ми рекомендуємо застосовувати при роботі з хмарною інфраструктурою Tucha:

- Прослідкуйте, аби для всіх облікових записів був увімкнений облік неправильних спроб введення паролю. Пам’ятайте про те, що обліковий запис користувача блокується на 1 годину після 5 неправильних спроб ввести пароль протягом 5 хвилин. Розблокувати облікові записи, що входять до групи «Адміністратори», можуть лише системні адміністратори. І здійснюється це після підтвердження того, що неправильний пароль був дійсно набраний самим користувачем. В іншому разі проблема передається службі інформаційної безпеки компанії.
- Не забувайте про регулярне оновлення пароля. Змінюйте його не рідше ніж один раз на 180 днів, а для облікових записів, які входять до групи «Адміністратори» — 1 раз на 90 днів.
- Якщо ви припускаєте, що хтось міг дізнатися ваш пароль, одразу ж змініть його та повідомте про це службу інформаційної безпеки компанії за телефоном або

на електронну пошту. У разі, якщо хтось вимагає від вас повідомити пароль, слід також одразу звернутися до нашої служби техпідтримки.

- Також негайно звертайтеся до служби безпеки компанії у разі, якщо ви загубили пароль, носій або пристрій, на якому він був збережений. Якщо хтось дізнався ваш пароль, ви самі можете змінити його.

Де і як правильно зберігати паролі

Розглянемо прості принципи зберігання паролів, які захистять ваші дані від потрапляння до рук зловмисників.

Як не слід зберігати паролі:

- не записуйте паролі в паперовій формі;
- не залишайте інформацію про паролі в будь-яких файлах або на носіях, доступ до яких є не тільки у вас;
- не зберігайте паролі, які були встановлені вам адміністраторами за замовчуванням;
- не зберігайте паролі в ПЗ, не призначеному для цього (в браузерах, утилітах підключення до інших сервісів тощо).

Для найбільш безпечного зберігання паролів ми рекомендуємо використовувати менеджери паролів, наприклад, KeePass, EnPass, CommonKey, Dashline тощо. А ще підготували для вас наочну інструкцію, як правильно налаштовувати і користуватися інструментом KeePass.

Резюме

Отже, захистити свої дані в інтернеті не так вже й складно. Важливо лише створити стійкий пароль, правильно його зберігати та дотримуватися простих заходів для захисту даних від доступу інших осіб. Тепер і ви знаєте, як це зробити. А якщо у вас виникли питання або ви припускаєте, що хтось міг дізнатися ваш пароль, звертайтеся до нас у будь-який час. Ми на зв’язку 24/7 і завжди надамо оперативну допомогу!

Джерело:

https://tucha.ua/uk/blog/instructions/yak-stvoriti-i-de-zberigati-nadiyniy-parol