Щомісячник з інформаційної безпеки для користувачів

OUCH!

У ЦЬОМУ НОМЕРІ…

Паролі

Підґрунтя

Паролі є чимось, що ви використовуєте майже кожен день, щоб отримати доступ до вашої електронної пошти та онлайн-банкінгу, купівлі товарів через мережу інтернет чи доступу до вашого смартфона. Однак паролі також є одним з ваших слабких місць, якщо хтось дізнається ваш пароль, вони можуть вкрасти вашу особистість, передати ваші гроші або отримати доступ до вашої особистої інформації. Надійні паролі мають важливе значення для захисту інформації. У цьому випуску ви дізнаєтеся, як створити надійні паролі, які легко запам'ятати за допомогою ключових фраз.

Гість номера

Гай Бруно - старший консультант з безпеки в IPSS Inc., інструктор в SANS та власник ISC. Гай має статус SANS GSE та закінчив программу SANS Cyber Guardian. Ви можете слідкувати за Гайем на Twitter за посиланням: **@GuyBruneau** та на сайті: **handlers.sans.org/gbruneau**.

Паролі

Завдання, з яким ми всі стикаємося, в тому, що кібер зловмисники розробили складні методи, щоб здогадатися, або підібрати паролі методом «грубої сили», і вони постійно удосконалюються. Це означає, що вони можуть поставити під загрозу ваші паролі, якщо вони слабкі або їх можна легко вгадати. Важливим кроком на шляху захисту інформації є використання надійних паролів. Чим більше символів у вашому паролі, тим він надійніше і його складніше підібрати. Однак довгі, надійні паролі важко згадувати. Тому, замість цього ми рекомендуємо вам використовувати ключові фрази, це прості фрази або речення, які легко запам'ятати, але важко зламати. Ось приклад:

Де цар Юліан?

Ця ключова фраза надійна не тільки завдяки довжині в 13 символів, але й тому, що використовує великі літери і символи (пам'ятаєте, пропуски і розділові знаки - це також символи). Ви можете зробити ваш пароль ще сильніше, якщо ви замініте букви з цифрами або символами, такі як заміна літери "А" з символом "@" або літеру "О" з числом нуль. Якщо веб-сайт або програма обмежує кількість символів, які можна використовувати в паролі, використовуйте максимальну дозволену кількість символів.

Безпечне використання паролів

Ви також повинні бути обережні, коли використовуєте ключові фрази. Використання ключової фрази не допоможе, якщо погані хлопці можуть легко вкрасти або скопіювати її.

Паролі

Використання надійних паролів є одним з найбільш ефективних кроків, які ви можете зробити, щоб захистити вашу особисту інформацію.

1. Обов'язково використовуйте різні паролі для кожного облікового запису та кожного пристрою, який у вас є. Наприклад, ніколи не використовуйте один і той же пароль для вашої роботи або банківського рахунку, який ви використовуєте для своїх власних обліковіх записів, таких як Facebook, YouTube або Twitter. Таким чином, якщо один з ваших рахунків скомпроментований, інші облікові записи у безпеці. Якщо у вас занадто багато паролів, які потрібно запам'ятовувати (що дуже поширено), подумайте про використання менеджера паролів. Це спеціальна програма, яка надійно зберігає всі ваші ключові фрази та паролі. Таким чином, використовуючи мереджер паролів ви будете повинні пам'ятати тільки пароль до вашого комп'ютера і програми менеджера паролів.

2. Нікому і ніколи не повідомляйте свій пароль, ключову фразу, або ваш особистий метод їх створення, в тому числі співробітникам. Пам'ятайте, ваш пароль, ключова фраза є вашою особистою таємницю. Якщо хтось, окрім вас знає ваш пароль він більше не є безпечним. Якщо ви випадково поділилися паролем з кимось ще, або, якщо ви вважаєте, що конфіденційність вашого паролю могла бути порушена або він вкрадений, змініть його негайно.

3. Уникайте використання поширенних слів та речень для ваших паролів та ключових фраз. Наприклад, фраза "Бджола мала, а й та працює" не кращий варіант для використання, так як вона добре відома.

4. Ніколи не використовуйте громадські комп'ютери, в готелях, бібліотеках, щоб отримати доступ до вашого робочого або банківського облікового запису. Будь-хто може використовувати ці комп'ютери, вони можуть бути заражені шкідливим кодом, який захоплює всі ваші натискання клавіш. Використовуйте тільки надійні та перевірені компьютери, щоб отримати доступ до власної конфіденційної інформації.

5. Будьте обережні, відвідуючи сайти, які вимагають, щоб ви надали відповіді на особисті питання. Ці питання використовуються, якщо ви забули ваш пароль і потрібні, щоб скинути його. Проблема в тому, що відповіді на ці питання часто можна знайти в Інтернеті, або навіть на вашій сторінці у Facebook. Переконайтеся в тому, що якщо ви відповісте на особисті питання ви використовуєте тільки інформацію, яка не є загальнодоступною або фіктивною. Менеджери паролів можуть допомогти вам з цим, так як дозволяють зберігати цю та іншу додаткову інформацію.

6. Багато інтернет-сервісів пропонують те, що називається двофакторною аутентифікацією, також відомою як двоступенева перевірка. Це де, наприклад вам потрібно використати не тільки пароль, а й код,

Паролі

який буде відправлений на ваш смартфон. Цей варіант є набагато більш безпечним, ніж використання простого паролю або ключової фрази. Кожен раз, коли це можливо, завжди використовувати ці надійні методи аутентифікації.

7. Мобільні пристрої часто вимагають використовувати PIN-код для захисту доступу до них. Запам'ятати PIN набагато легше, ніж звичайний пароль. Чим довший ваш PIN-код, тим він безпечніше. Багато мобільних пристроїв дозволяють використовувати ключову фразу замість PIN-коду.

8. І, нарешті, якщо ви більше не використовуєте обліковий запис, не забувайте видалити або заблокувати його.

About Crytek

Crytek is an independent videogame developer, publisher and technology provider with headquarters in Frankfurt am Main (Germany) and seven other studios around the world. Established in 1999, Crytek has created multiple award-winning titles, including the original Far Cry, the Crysis series, Ryse: Son of Rome and Warface. All of Crytek's games are developed using CRYENGINE, the company's cutting-edge 3D game technology, which is also the first choice of other leading developers and licensees when creating games for PC, Xbox One, PlayStation®4, Wii UTM, iOS and Android. Crytek's ongoing growth in the games-as-a-service market has extended the company's reach as they continue to deliver top quality interactive experiences to players through self-publishing platforms online.

ДІЗНАЙТЕСЯ БІЛЬШЕ

Підпишіться на OUCH! - Щомісячний журнал з інформаційної безпеки, отримаєте доступ до архівів OUCH! і дізнайтеся більше про рішення SANS в питаннях інформаційної безпеки на нашому сайті: http://www.securingthehuman.org.

Ресурсы

Двоступенева перевірка:	http://www.securingthehuman.org/ouch/2013#august2013
Менеджери паролів:	http://www.securingthehuman.org/ouch/2013#october2013
Соціальна інженерія:	http://www.securingthehuman.org/ouch/2014#november2014
Термінологія компьютерної безпеки:	http://www.securingthehuman.org/resources/security-terms

Редакція: Білл Вайман, Уолт Скрівенс, Філ Хоффман, Боб Рудіс
Український переклад: Дмитро Коржевін