This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-sa/3.0/

Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Una hora de ciencia

Como elegir el nombre de tu perro
(o la importancia de las contraseñas)

Febrero 22, 2008

ERA DIGITAL Y DE LA INFORMACIÓN

Breve Introducción a la SI

- Identificación
- **Autenticación**
- Autorización

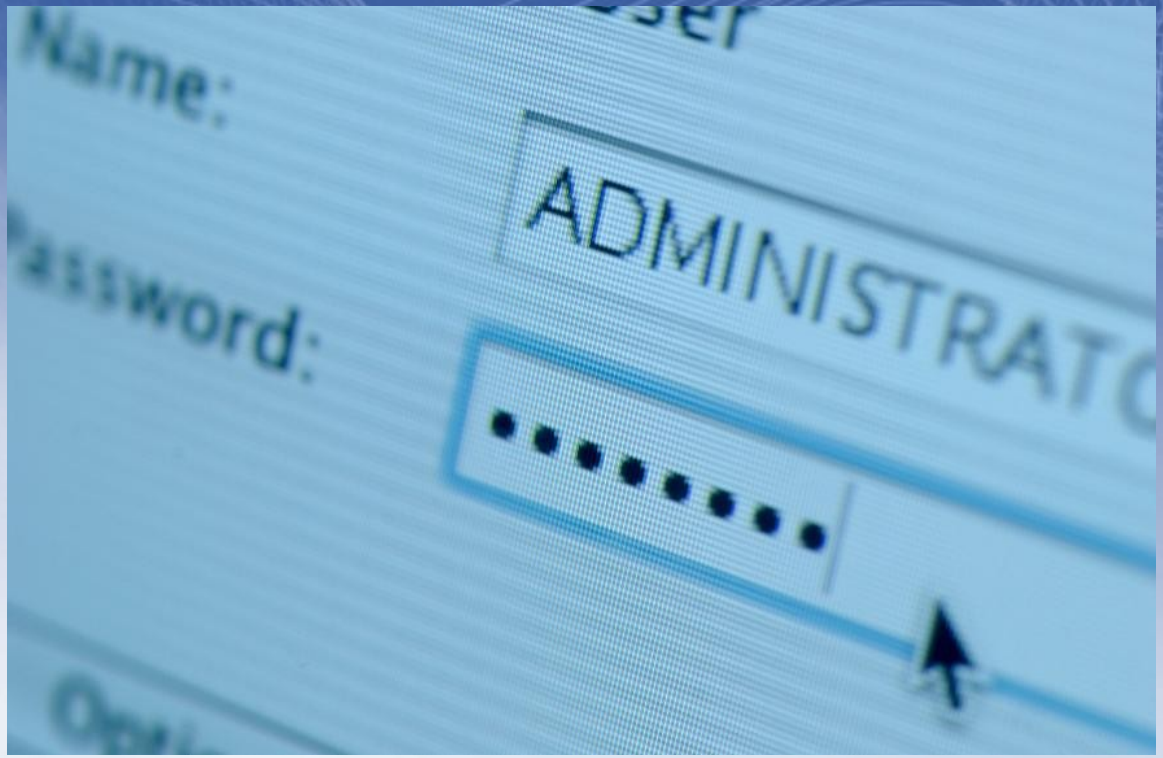
Algo que tengo

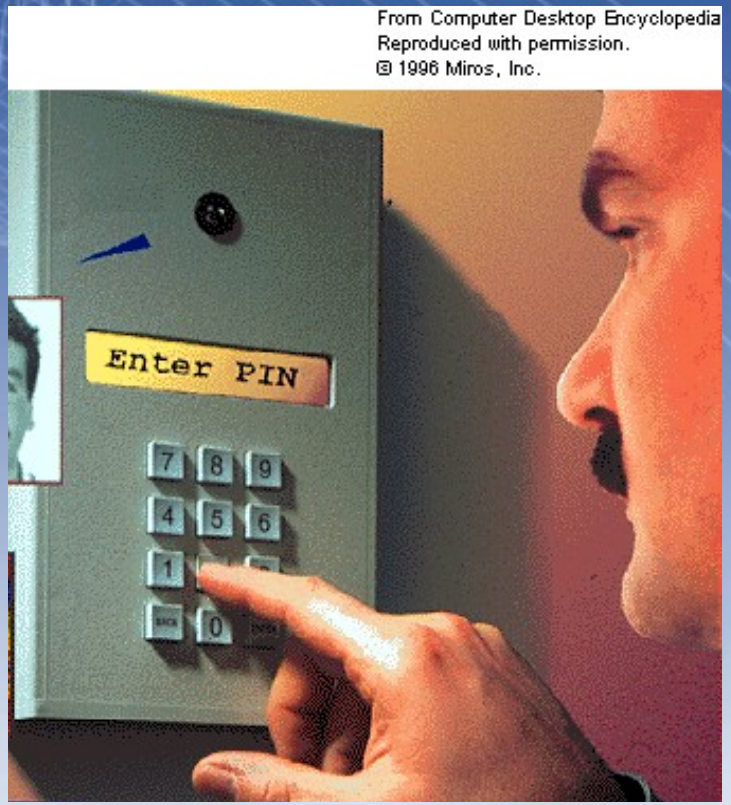
RSA SecurID SD600

RSA SecurID SID700

Algo que soy

Algo que sé


Name:
ADMINISTRATO
Password:


From Computer Desktop Encyclopedia
Reproduced with permission.
© 1996 Miros, Inc.
Enter PIN

Contraseñas

- Algo que se.
- Baratas, fáciles de implementar, MUY USADAS
- Problema:
  - Esta demostrado que los humanos no recordamos contraseñas con alta **entropia**

Robo de Información famoso

Getting Started | Honeynet Project RS... | honeyblog | El Universal: Minuto... | OSNews | Barrapunto | La Cofradia Digital

paris hilton ... | paris hilton ... | Google Ima... | Google Ima... | Google Ima... | Paris Hilt... | Loading...

On ZDNet: 100 GB memory chip next year

c|net NEWS.com

Search: News Go Advanced search

Today on CNET | Reviews | News | Downloads | Tips & Tricks | CNET TV | Compare Prices | Blogs

Business Tech | Cutting Edge | Green Tech | Wireless | Security | Media | Markets | Personal Tech | News Blogs | Video | Extra | My News

Paris Hilton's cell phone hacked?

By Steven Musil

paris hilton hacked - Google... | paris hilton phone hacked - ... | Paris Hilton's cell phone hac... | Teen Pleads Guilty to H...

washingtonpost.com Sign In | Register Now

The Washington Post Print Edition | Subscribe

NEWS | POLITICS | OPINIONS | LOCAL | SPORTS | ARTS & LIVING | CITY GUIDE | JOBS | CARS | REAL ESTATE | RENTALS | SHOPPING

SEARCH go washingtonpost.com Web Results by Google | Search Archives

Advertisement

washingtonpost.com > Technology > Special Reports > Cyber-Security

TechNews.com

Print This Article

E-Mail This Article

Teen Pleads Guilty to Hacking Paris Hilton's Phone

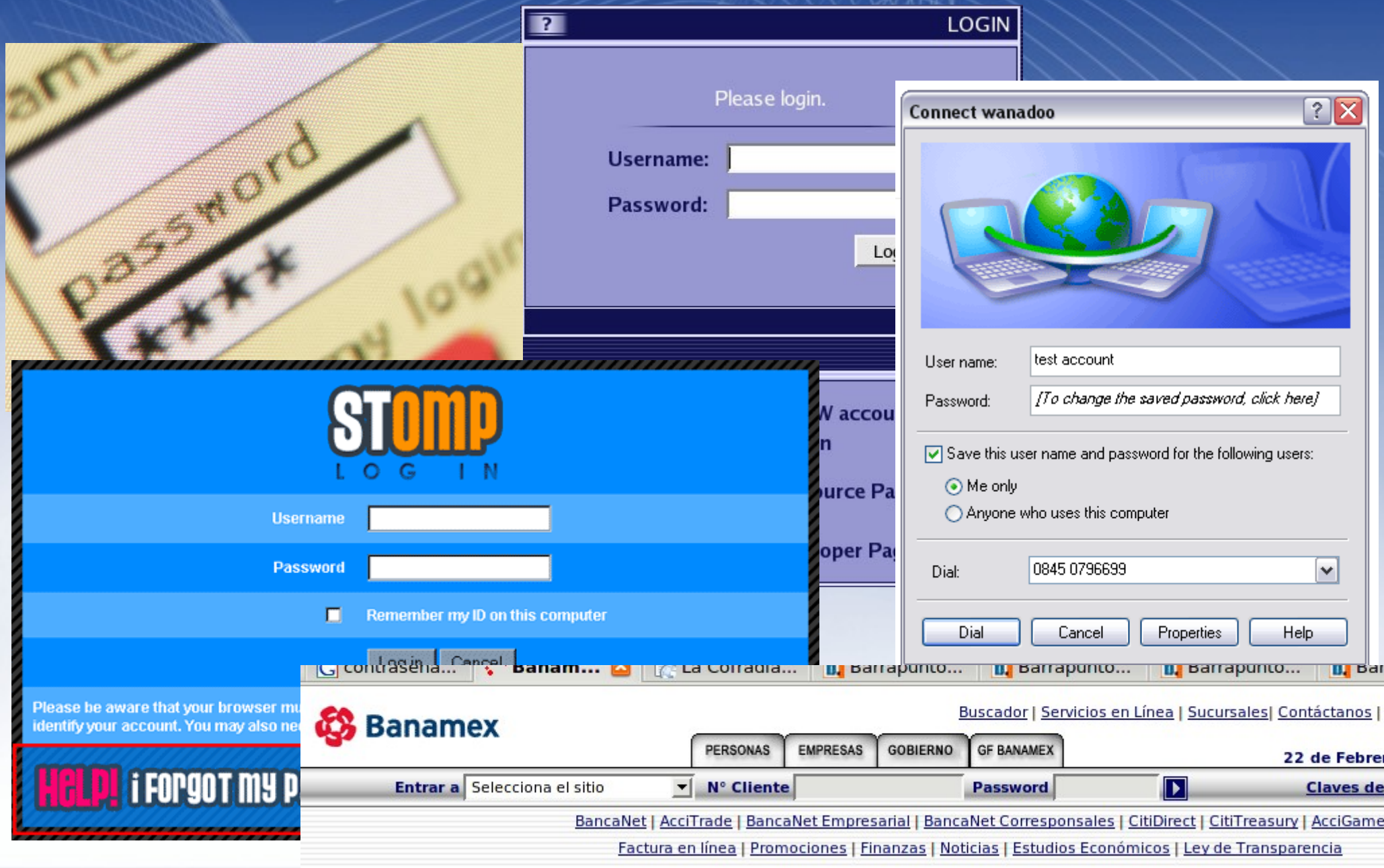
By Brian Krebs

washingtonpost.com Staff Writer

Advertisement

3.60%

Usos de la contraseña



Cómo eliges tu contraseña

123456

asdfghj

Calidad de las contraseñas

Recomendaciones

- Más de 8 caractéres
- Uso de almenos 3 de los siguientes:
  - Mayúsculas
  - Minúsculas
  - Números
  - Símbolos
- No palabras comunes o de diccionario
- Políticas de cambio frecuente,
  - No reutilización ni contraseñas parecidas

Medir la entropía

- La entropía mide que tanta información nos brinda una variable
- 0 -> ninguna información
- A mayor entropía mayor calidad de la contraseña
- $e = \sum_{1}^{n} p(n) * \log_{2}(p(n))$

Medir la calidad

- Muchos esquemas se basan en cuanto tiempo se puede crackear la contraseña ...
  - Ataques de diccionario
  - Modificaciones al diccionario
  - Ataques de fuerza bruta
- A mayor tiempo mejor es la contraseña
- A mayor espacio de búsqueda de la contraseña, más tiempo es necesario para romperla

Probabilidades de letra siguiente

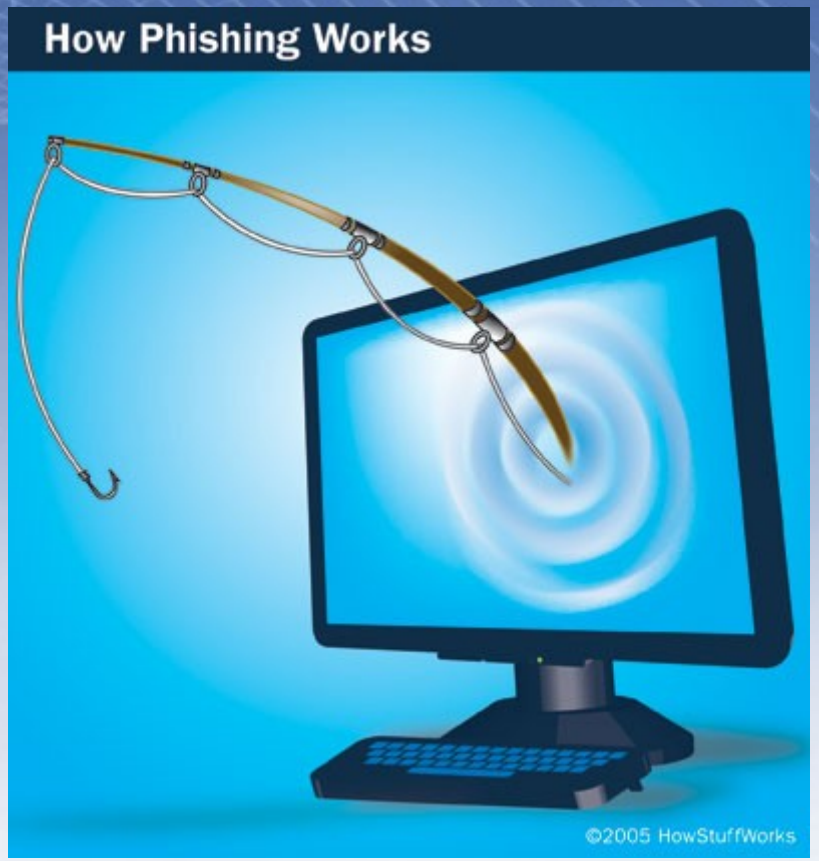
- Es dificil recordar caracteres completamente aleatorios
- Medir la probabilidad de que la letra que sigue sea *a* o *b* dependiendo de la actual -> generar diccionarios más extensos
- Si la probabilidad de la letra siguiente es alta, la calidad de la contraseña baja

Donde se usa la calidad de las contraseñas ?

- Para definir políticas de generación de contraseñas.
- Proactive password checkers

Ataques posibles

- Diccionario
- Fuerza bruta
- **Phishing scam**
- **Ingeniería Social**



Recomendaciones

- ~~Usar generadores de contraseñas seguras~~
- ~~Usar frases en lugar de contraseñas~~
- Tomas una frase fácil de recordar
- Escribes los principios de cada palabra
- Intercambias algunas letras por números o símbolos

ejemplo

- La verdad nos hará libres
- lavernhali
- 7av3rn#al1

- Segura y “fácil” de recordar

Proyecto propuesto

- Desarrollar un medidor de calidad de contraseñas.
  - Usando entropía
  - Diccionarios
  - Secuencias
  - Distancia de edición de Levenshtein
  - Otras recomendaciones

Ultimas recomendaciones

Más usadas en la UPSLP

- sergio
- alejandra
- castillo
- 123456
- 123456789
- 12345
- estrella

Preguntas