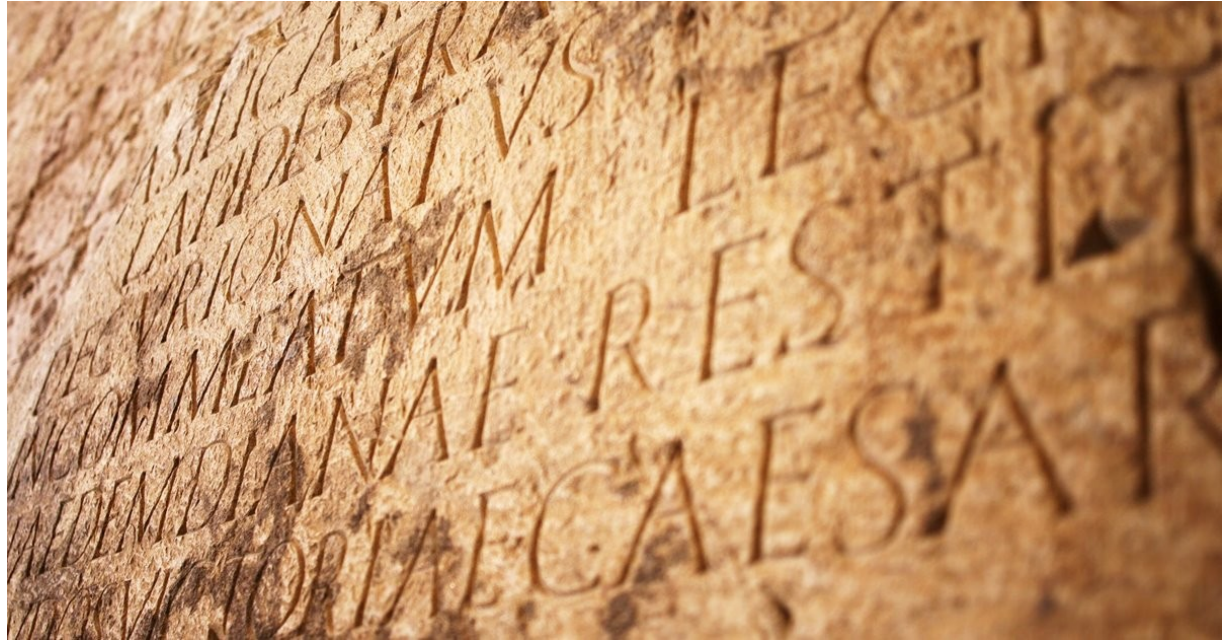


¿Qué son y qué hacen las contraseñas?



Una contraseña o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

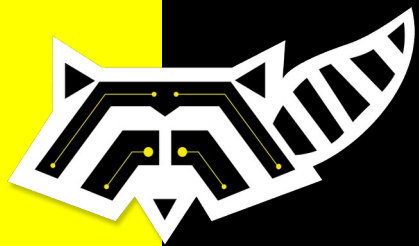




Las contraseñas cumplen con dos objetivos fundamentales:

- Sirven como medio para autenticar nuestra identidad al tratar de ingresar a un servicio determinado.
- Permiten el acceso a información que de otro modo, es decir, sin las credenciales correctas, es inaccesible, tal como sucede con una llave y una cerradura.





La Teoría de Contraseñas



Dos tipos de contraseñas

- ☐ Contraseñas que **se comparan** para verificar acceso
 - ☐ Contraseñas que **son** la llave mismo
-



¿Dónde se usan las contraseñas?

- ☐ Casi todas las contraseñas son usadas para sitios web.
 - Estas son del tipo de comparación
 - ☐ El sitio web va a guardar tu contraseña
 - En ocasiones, estas se hashearán
 - ☐ Esto significa que pueden ser sobreescritas o robadas
-



¿Dónde se usan las contraseñas?

- ☐ Casi todos los computadores tienen contraseñas para las cuentas de usuarios
 - Estas también son del tipo de comparación
 - ☐ Entonces, alguien con acceso a tu disco duro podría acceder al contenido sin contraseña
-



¿Dónde se usan las contraseñas?

- ☐ Los discos duros cifrados utilizan contraseñas que **son** la llave
 - ☐ También los gestores de contraseñas,
 - ☐ Archivos zip cifrados
 - ☐ Y documentos cifrados
 - ☐ En general, este tipo de acceso no requiere un usuario
-



¿Cómo se atacan las contraseñas?

- La forma más fácil se llama *fuerza bruta*
 - Se prueban todas las combinaciones
 - Pero si se trata de un sitio web, cada intento va a demorar segundos
 - Y casi todos los sitios web van a bloquear el acceso después de unos intentos
-



¿Cómo se atacan las contraseñas?

- Imaginen que tienen una contraseña con 6 caracteres, compuesta de letras mayúsculas, minúsculas y dígitos
 - Esto significa $26 + 26 + 10$ posibilidades, que son 62 en total
 - 6 caracteres significa $62^6 = 56,800,235,584$ posibilidades
-



¿Cómo se atacan las contraseñas?

- ❑ 56,800,235,584 intentos en un sitio web, cuando cada intento demora 1 segundo, significa 15,777,843 horas o 657,410 días, o casi 1800 años
 - ❑ Pero, si alguien roba la base de datos y puede intentar 100,000 combinaciones cada segundo, son sólo 6.5 días
-



¿Cómo se atacan las contraseñas?

- Con un computador razonablemente potente, y si la base de datos guarda las contraseñas con SHA-1, herramientas actuales pueden probar más de 2,000,000,000 contraseñas cada segundo
-



¿Cómo se atacan las contraseñas?

- ☐ Otra manera de atacar contraseñas es buscando contraseñas que ya hayan sido filtradas y probarlas
 - ☐ También se puede combinar este método con otros procedimientos
-



¿Cómo se atacan las contraseñas?

- ☐ Finalmente, se puede adivinar contraseñas basándose en información sobre la persona, listas de palabras, la estructura de oraciones, textos conocidos de libros, etc
-



Buenas contraseñas

- ☐ **No** tienen estructura
 - ☐ Tienen un **gran cantidad** de aleatoriedad
 - ☐ No pueden ser *crackeadas*, aunque sepas cómo están construidas
 - ☐ No se pueden recordar
-



Buenas contraseñas

- ☐ No es posible que los seres humanos las generen
 - ☐ Pueden ser generadas con dados y listas de palabras
 - ☐ O un computador
-



Buenas contraseñas

- ☐ No mejoran significativamente aumentando de 8 a 9 caracteres
- ☐ Ni con agregar caracteres especiales como & o %



Dos tipos de contraseñas buenas

- ☐ Aquellas que **necesitas** recordar
 - Por ejemplo, la que usas para tu ordenador
 - ☐ Y las que no
 - Como las contraseñas para sitios web
-



Dos tipos de contraseñas buenas

- Para contraseñas que no necesitas recordar:
 - Usa un gestor de contraseñas para guardarlas
 - Usa el generador en el gestor de contraseñas para generar una contraseña con el tamaño máximo
-



Dos tipos de contraseñas buenas

- Para contraseñas que necesitas recordar:
 - Usa el método **Diceware**
 - Usa 5 a 8 palabras, dependiendo de tus necesidades de seguridad
-



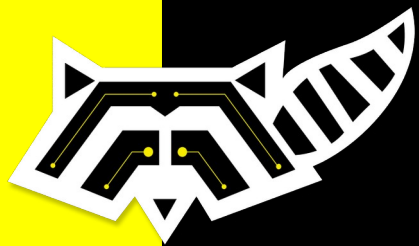
Diceware

- ☐ Descarga una lista de palabras
 - ☐ Usa 5 dados para escoger una palabra
 - ☐ Repite hasta que tengas palabras suficientes.
 - ☐ Combina las palabras, separándolas con espacios, en minúscula, para tu contraseña.
 - ☐ Esta será fácil de recordar.
-



La seguridad de Diceware

- Considerando que la lista de palabras en general contiene 7776 palabras, significa que una palabra implica 7776 posibilidades.
 - 5 palabras significa 7776^5 posibilidades, que es 28,430,288,029,929,701,376
 - Que significa más o menos 901 mil millones de años para adivinar tu contraseña – con un intento cada segundo.
-



Robustez

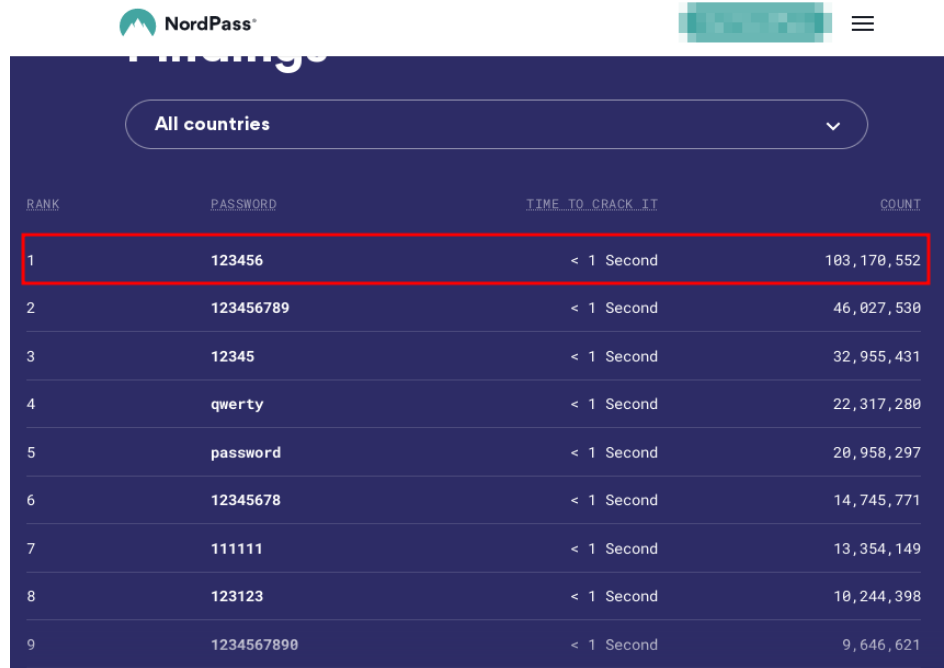


Keeper – 25 millones de contraseñas



National Cyber
Security Centre

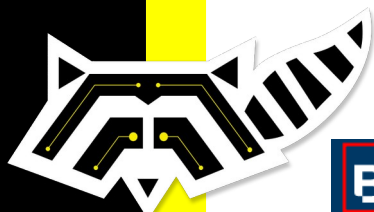
100 millones de contraseñas



The screenshot shows the NordPass interface with a list of common passwords. The first row is highlighted with a red border.

RANK	PASSWORD	TIME_TO_CRACK_IT	COUNT
1	123456	< 1 Second	183,170,552
2	123456789	< 1 Second	46,027,530
3	12345	< 1 Second	32,955,431
4	qwerty	< 1 Second	22,317,280
5	password	< 1 Second	20,958,297
6	12345678	< 1 Second	14,745,771
7	111111	< 1 Second	13,354,149
8	123123	< 1 Second	10,244,398
9	1234567890	< 1 Second	9,646,621

Más de 4 TB de información analizada



PROMOCIONES

CALCULADORAS

SUSCRIBIRSE

Crear contraseñas robustas

Al momento de crear claves seguras, la recomendación es implementar una longitud mínima de ocho caracteres, combinando mayúsculas con minúsculas y símbolos con números.

Asimismo, evitar el uso de: nombres propios, números consecutivos, cualquier número de celular, fechas especiales o letras consecutivas del teclado.

BBVA

Contraseñas seguras: consejos para proteger los datos personales y financieros

Consejos:

- Crearlas con al menos 8 caracteres, que incluyan números, letras mayúsculas y minúsculas y caracteres especiales.

Contraseñas seguras - Seguridad online Banco Santander (2015)

#SantanderSeguridad

Se recomienda usar un mínimo de 6 caracteres

Rx48#N

Elige contraseñas difíciles de averiguar.

MORE VIDEOS

Ayuda de Cuenta de Google



Describe tu problema



Crear una contraseña más extensa y que puedas recordar mejor

Las contraseñas largas son más seguras: asegúrate de que la tuya tenga 12 caracteres como mínimo. Estas sugerencias pueden ayudarte a crear contraseñas más largas y que sean más fáciles de recordar. Intenta usar:

- La letra de una canción o un poema
- Una cita significativa de una película o un discurso
- Un pasaje de un libro
- Una secuencia de palabras que te resulten significativas
- Una abreviatura (crea una contraseña con la primera letra de cada palabra de una oración)

No elijas contraseñas que puedan ser fáciles de adivinar para:

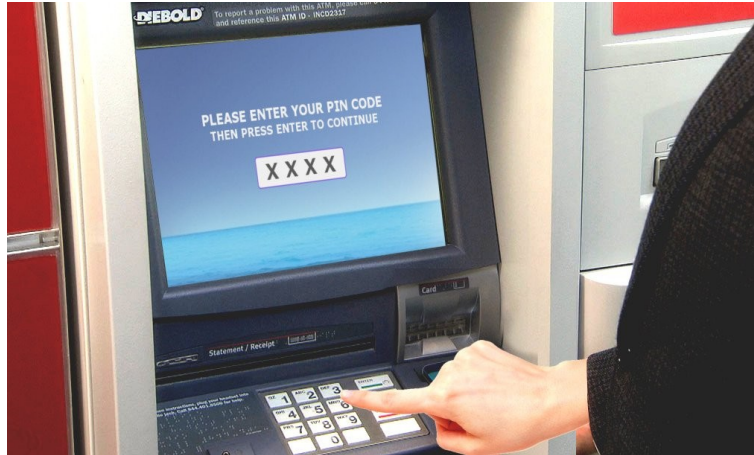
- Personas que te conocen
- Personas que busquen información de fácil acceso (como tu perfil en redes sociales)



Fortaleza

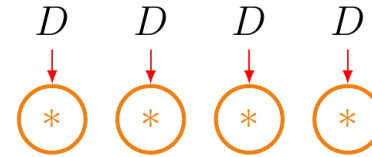


El número de potenciales variaciones que un atacante necesita intentar para encontrar la contraseña correcta.



$$D = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

$$\#D = 10$$



$$10 \times 10 \times 10 \times 10 = 10^4 = 10000$$



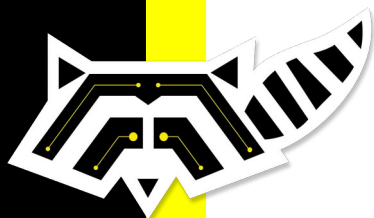
¿Cómo fortalecer la contraseña?

¿Aumentar la longitud de la contraseña?

$$10^6 = 1.000.000$$

¿Aumentar la tamaño del conjunto con el cual se contruye la contraseña? (D)

Alfabeto inglés (26 símbolos) + números dígitos (10 símbolos): $36^4 = 1.679.616$



Entropía

$$\log_2 N^L$$

Es una medida de la incertidumbre y la información necesaria para que cualquier proceso logre reducir o eliminar la incertidumbre



L05 NUM3R05 PU3D3N U71L1Z4R53 C0M0 L37R45, Y L4
FR453 R35ULT4NT3 PU3D3 53R L31D4 51N MUCH0
35FU3RZ0

Esta noche ? las ? arder bajo ? ? del ?

Caminando ? casa encontré ? flor ? la ? vi reflejada ?
sonrisa



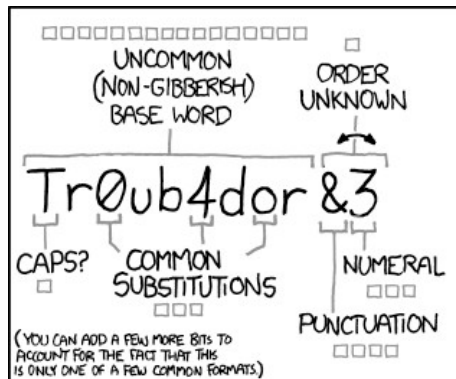
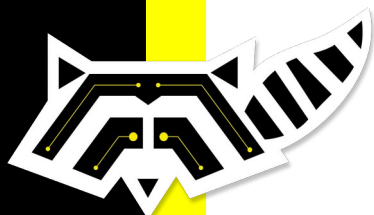
¿Cómo crear una buena contraseña?

32125	guise	32255	hair	32425	have	32555	hemp
32126	guitar	32256	hairy	32426	haven	32556	hen
32131	gules	32261	haiti	32431	havoc	32561	hence
32132	gulf	32262	hal	32432	haw	32562	henri
32133	gull	32263	hale	32433	hawk	32563	henry
32134	gully	32264	haley	32434	hay	32564	her
32135	gulp	32265	half	32435	haydn	32565	hera
32136	gum	32266	halma	32436	hayes	32566	herb
32141	gumbo	32311	halo	32441	hazard	32611	herd
32142	gummy	32312	halt	32442	haze	32612	here
32143	gun	32313	halvah	32443	hazel	32613	hero
32144	gunk	32314	halve	32444	hazy	32614	heroic
32145	gunny	32315	ham	32445	hb	32615	heron
32146	gunny	32316	hamal	32446	hc	32616	herr
32151	gurgle	32321	hamlin	32451	hd	32621	hertz
32152	guru	32322	han	32452	he	32622	hess
32153	gus	32323	hand	32453	he'd	32623	hesse
32154	gush	32324	handy	32454	he'll	32624	hettie
32155	gust	32325	hane	32455	head	32625	hetty
32156	gusto	32326	hang	32456	heady	32626	hew
32161	gut	32331	hank	32461	heal	32631	hewitt
32162	gutsy	32332	hanna	32462	healy	32632	hewn
32163	guy	32333	hanoi	32463	heap	32633	hex
32164	guyana	32334	hans	32464	hear	32634	hey
32165	gv	32335	hansel	32465	heard	32635	hf
32166	gw	32336	hap	32466	heart	32636	hg
32211	gwen	32341	hard	32511	heat	32641	hh
32212	gwyn	32342		32512	heath	32642	hhh
32213		32343		32513		32643	hhhh



segundos / año = 31557600
intentos / segundo = 10000
entropía = $\log_2(7776^6) \approx 77$

aprox. 700.540.978.150 años



~28 BITS OF ENTROPY

□□□□□□□□ □
□□□□□□□□ □
□□□ □□□
□□□□ □


$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

(PLAUSIBLE ATTACK ON A WEAK REMOTE
WEB SERVICE. YES, CRACKING A STOLEN
HASH IS FASTER, BUT IT'S NOT WHAT THE
AVERAGE USER SHOULD WORRY ABOUT.)

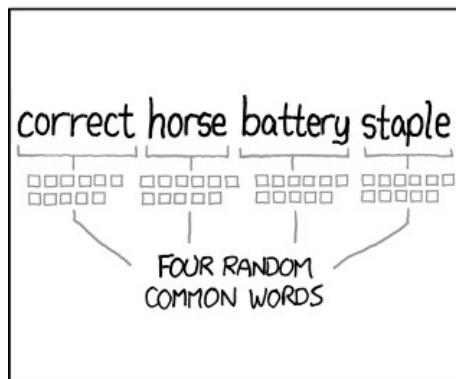
DIFFICULTY TO GUESS:
EASY

WAS IT TROMBONE? NO,
TROUBADOR. AND ONE OF
THE 0s WAS A ZERO?

AND THERE WAS
SOME SYMBOL...



DIFFICULTY TO REMEMBER:
HARD



~44 BITS OF ENTROPY

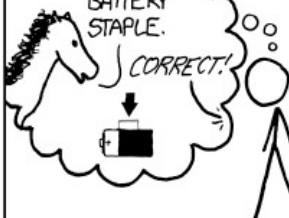
□□□□□□□□ □□□□□□□□
□□□□□□□□ □□□□□□□□
□□□□□□□□ □□□□□□□□
□□□□□□□□ □□□□□□□□

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS:
HARD

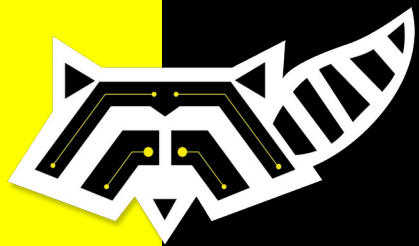
THAT'S A
BATTERY
STAPLE.

CORRECT!



DIFFICULTY TO REMEMBER:
YOU'VE ALREADY
MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED
EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS
TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Errores comunes en el manejo de contraseñas



La lista completa

1. 123456	14. login
2. password	15. abc123
3. 12345678	16. starwars
4. qwerty	17. 123123
5. 12345	18. dragon
6. 123456789	19. passw0rd
7. letmein	20. master
8. 1234567	21. hello
9. football	22. freedom
10. iloveyou	23. whatever
11. admin	24. qazwsx
12. welcome	25. trustno1
13. monkey	

- Utilizar referencias personales para la creación de nuestras contraseñas.
 - Crear contraseñas demasiado simples.
 - Utilizar las mismas contraseñas para todas nuestras cuentas en distintos servicios.
-



- Crear contraseñas con pequeñas variaciones para distintas cuentas.



GmailCarlos84



TwitterCarlos84



FacebookCarlos84



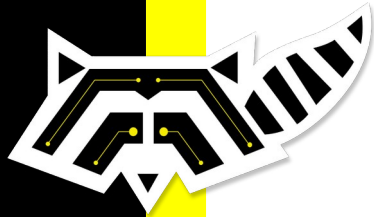
NetflixCarlos84



InstagramCarlos84



SRICarlos84



- Usar las contraseñas sugeridas por las plataformas digitales.



Paso 4

Crea y personaliza tu nuevo nombre de usuario y contraseña.

- **Usuario:** Máximo 16 y mínimo 8 caracteres. Debe ser alfanumérico, puedes usar mayúsculas, minúsculas, números y caracteres especiales permitidos (punto; guion; subguion).
- **Contraseña:** Máximo 12 y mínimo 8 caracteres. Debes usar mayúsculas, minúsculas, números y caracteres especiales, debes cumplir al menos 3 de estas condiciones.





Para que nuestra
contraseña sea **segura**,
podemos leer estas **sugerencias**

Transferencia Express

INTERNAS ☒ EXTERNAS

MAYAXXXXX XXXXXCELA XXXX XXXX

Seleccione la cuenta del beneficiario

MONTO (Ej: 2,357.82)

ACEPTAR CANCELAR

Recargas

Modificar Contraseña

JuanMaya6292

CONTRASEÑA NUEVA

Contraseña Fuerte

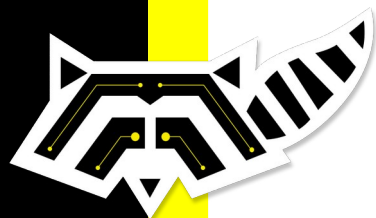
CONFIRMAR CONTRASEÑA

Sugerencias para la elección de la contraseña

- La contraseña nueva debe tener de 8 a 15 caracteres
- Deben incluirse mayúsculas, minúsculas y números
- Ejemplo de una contraseña de nivel de seguridad fuerte:**
Ulw6Ab_AB@

ACTUALIZAR CANCELAR

Cooperativa Juventud Ecuatoriana Progresista
Todos los derechos reservados - 2016



Inscríbete

Debes inscribirte para disfrutar de todas las ventajas que te ofrece Capacitate para el empleo, tales como:

- Historial de tus calificaciones.
- Perfil personalizado.
- Comprobante de estudios.

Proporciona los datos que te pedimos a continuación. Todos los datos marcados con (*) son requeridos.

¡Así de fácil es crear tu cuenta!

Tu nombre ●

Maritza

Tus apellidos ●

Vizcaino

Eres... ●

Mujer

¿Cuántos años has asistido a la escuela? ●

17

Idioma preferido ●

Español

Mes en el que naciste ●

Julio

Año en el que naciste ●

1957

País donde vives ●

Ecuador

Estado/Departamento/Provincia ●

Pichincha

Municipio

Selecciona un municipio

Código Postal (opcional)

470525

Use una contraseña generada de forma seg.

uj iVYnN35c4WMMt

Firefox va a guardar esta contraseña para este sitio web.

Ver inicios de sesión guardados

[Ver]

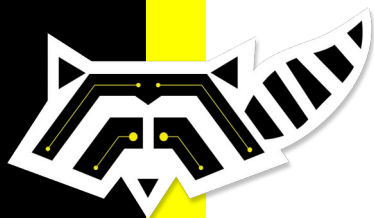
¿Podemos contactarte con ofertas de empleo? ●

--Selecciona una opción--

Use una contraseña generada de forma seg.
uj iVYnN35c4WMMt

Firefox va a guardar esta contraseña para este sitio web.

Ver inicios de sesión guardados



- Utilizar contraseñas que ya han sido objeto de filtraciones.

```
45. sharon.carpenter@ci.minneapolis.mn.us adam12
46. anne.fischer@ci.minneapolis.mn.us junositka
47. annie.barrett@ci.minneapolis.mn.us louisel581
48. annie.boone@ci.minneapolis.mn.us flipper
49. william.woodis@ci.minneapolis.mn.us woody320
50. valerie.thompson@ci.minneapolis.mn.us renoir2009
51. tammy.diedrich@ci.minneapolis.mn.us TammyMN
52. raymond.cruz@ci.minneapolis.mn.us july72214
53. todd.gillmeister@ci.minneapolis.mn.us cowboys
54. tom.crawford@ci.minneapolis.mn.us mookie
55. curt.fernandez@ci.minneapolis.mn.us Audin666
56. cynthia.govan@ci.minneapolis.mn.us friday
57. joan.hammell@ci.minneapolis.mn.us hotdog
58. jodie.koenig@ci.minneapolis.mn.us Sprite326
59. aaron.hanauer@ci.minneapolis.mn.us Parking1
60. adam.grobove@ci.minneapolis.mn.us Mpd02486
61. craig.worrell@ci.minneapolis.mn.us kSaGsRj64E
62. pat.wheeler@ci.minneapolis.mn.us 055123p
63. patrick.windus@ci.minneapolis.mn.us martin69
64. patt.keane@ci.minneapolis.mn.us convention
65. patti.stclair@ci.minneapolis.mn.us 96491
66. ricardo.cervantes@ci.minneapolis.mn.us Xavier
67. richard.christensen@ci.minneapolis.mn.us chris7949
68. richard.heim@ci.minneapolis.mn.us 1603
69. leaann.stagg@ci.minneapolis.mn.us lamsCK
70. lee.peterson@ci.minneapolis.mn.us leedps
71. nickolas.vangunst@ci.minneapolis.mn.us ivan01
72. brandon.kitzerow@ci.minneapolis.mn.us smwpadt
73. brenda.shepherd@ci.minneapolis.mn.us thekids
74. brian.karkula@ci.minneapolis.mn.us brutus
75. stephen.norton@ci.minneapolis.mn.us cityattorn
76. samantha.lavoie@ci.minneapolis.mn.us jasmine
```

```
73. brenda.shepherd@ci.minneapolis.mn.us thekids
74. brian.karkula@ci.minneapolis.mn.us brutus
75. stephen.norton@ci.minneapolis.mn.us cityattorn
76. samantha.lavoie@ci.minneapolis.mn.us jasmine
77. sandra.anderson@ci.minneapolis.mn.us u5obhpk2r7an
78. sandra.kellogg@ci.minneapolis.mn.us zelda1
79. sandy.jackson@ci.minneapolis.mn.us jackssa0
80. Anthony.Miranda@ci.minneapolis.mn.us wemlinger
81. BARBARA.JOHNS@CI.MINNEAPOLIS.MN.US petersen
82. Christopher.Hudok@ci.minneapolis.mn.us 134302785966793
83. Constance.Leaf@ci.minneapolis.mn.us 01roscoe
84. Dale.Burns@ci.minneapolis.mn.us defense
85. Dale.Cannon@ci.minneapolis.mn.us thebosss
86. Dana.Davis@ci.minneapolis.mn.us bubba29
87. Dave.Stoppelman@ci.minneapolis.mn.us sirw3567
88. Debra.Parker@ci.minneapolis.mn.us de53bby
89. Duane.Nygren@ci.minneapolis.mn.us 758068353703847
90. Dwaine.Culliton@ci.minneapolis.mn.us Elevator
91. GREGORY.LANGFORD@ci.minneapolis.mn.us password
92. Inger.Millard@ci.minneapolis.mn.us myobama
93. Jeff.Handeland@ci.minneapolis.mn.us P1c@rd
94. Jeff.Kendall@ci.minneapolis.mn.us jackson5
95. Jeffrey.Metzen@ci.minneapolis.mn.us metz1287
96. Joyce.Traver@ci.minneapolis.mn.us lauren@21
97. Leslie.Tevling@ci.minneapolis.mn.us brodie22
98. Lucy.McAlpine@ci.minneapolis.mn.us 535353
99. Lynn.Schwartz@ci.minneapolis.mn.us HelenL
100. Magdy.Mossaad@ci.minneapolis.mn.us Magdy56
101. Matthew.StGeorge@ci.minneapolis.mn.us midget454
102. Michael.Seide@ci.minneapolis.mn.us 841368510222674
103. Mike.Hestick@ci.minneapolis.mn.us linkedin
```



- Guardar nuestras contraseñas en el navegador al acceder a algún servicio.

A screenshot of a Firefox browser window. The address bar shows the URL <https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=13>. A modal dialog box is displayed over the page content, titled "¿Guardar el inicio de sesión para live.com?". It contains a "Nombre de usuario" field with a dropdown menu showing "@hotmail.com", a "Contraseña" field with masked characters (dots), and a checkbox labeled "Mostrar contraseña". At the bottom right of the dialog are two buttons: "No guardar" and "Guardar".

Firefox

Cuenta Microsoft

← → ↻ 🔒 🔓 🔑 <https://login.live.com/ppsecure/post.srf?wa=wsignin1.0&rpsnv=13>

¿Guardar el inicio de sesión para live.com?

Nombre de usuario

@hotmail.com

Contraseña

●●●●●●

☐ Mostrar contraseña

No guardar Guardar



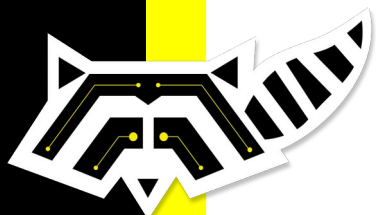
- Compartir contraseñas con otras personas.
- Usar contraseñas en dispositivos no seguros.



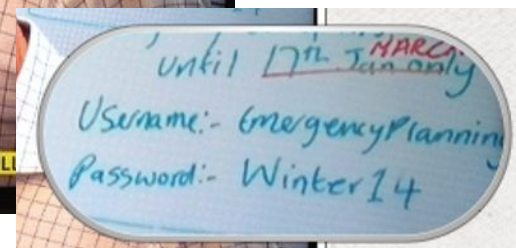


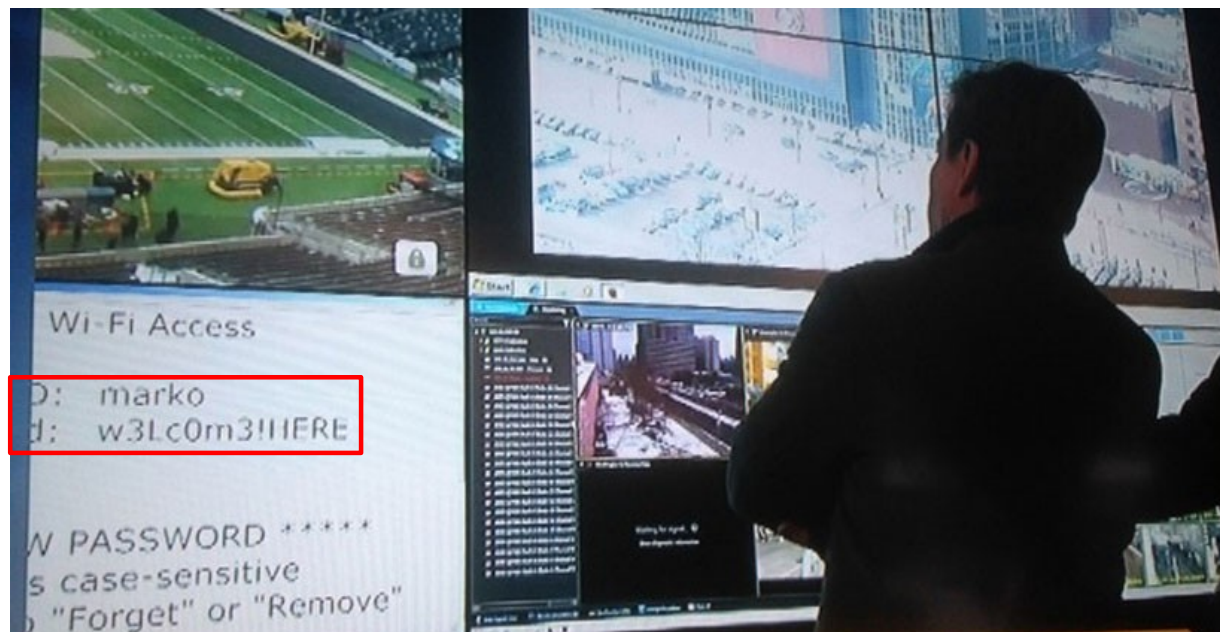
- Ingresar tu contraseña frente o cerca a una cámara.



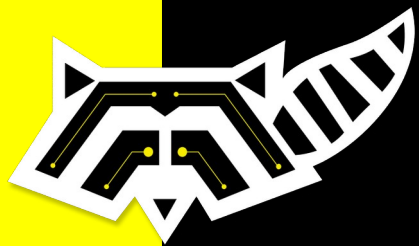


- Apuntar nuestras contraseñas.









Gestores de Contraseñas



ONLANE



Preguntas

Centro de Autonomía Digital
