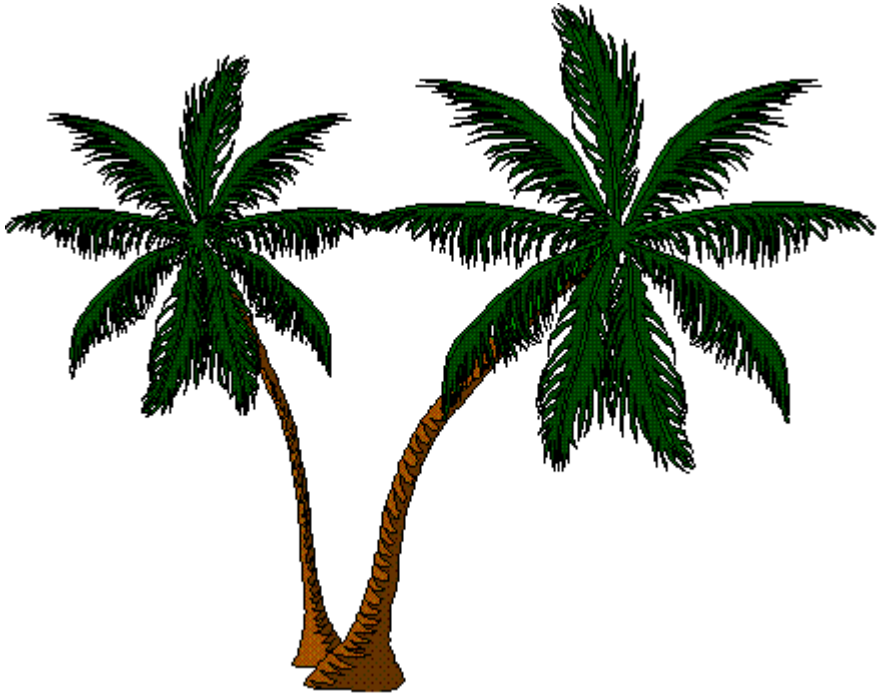
Sobreviviendo en la jungla



Seguridad en cómputo
2018

Seguridad: ¡Siempre!

- “Cuando yo tenia tu edad...”
- La red es hostil
- ¡***Tu red*** es hostil!

Seguridad: ¿Por qué?

- Tus datos
- Tus computadoras
- Tu paz mental

Un poquito de paranoia

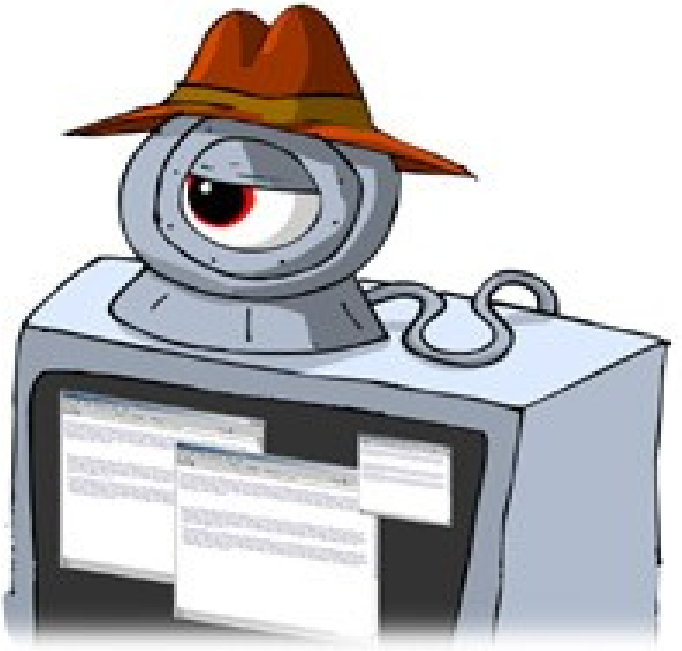
- La seguridad no es algo que se hace una sola vez y se olvida
- Paranoia: Necesaria pero con perspectiva

Aspectos de la seguridad

- **Externa**
- **Interna**
  - Datos
  - Seguridad física
  - Ingeniería social

Seguridad externa

- ¡Es la mas famosa!
- **Hábito:** Mantenerte actualizado
- **Costumbre:** Informarse siempre
- **Método:** La lista



Seguridad externa: actualízate

- Ningún software es perfecto
- Un sistema actualizado es un sistema seguro
- En Software Libre los problemas se solucionan rápido

Seguridad externa: Infórmate

- **CVE**
  (cve.mitre.org)
- **UNAM-CERT**
  (www.seguridad.unam.mx)
- **Sitios de la comunidad**
  (news.ycombinator.com)
- **Twitter, facebook**

  (@unamcert)

El gusano morris

http://securitydigest.org/phage/archive/383

Wed, 2 Nov 88 23:28:00 PST:

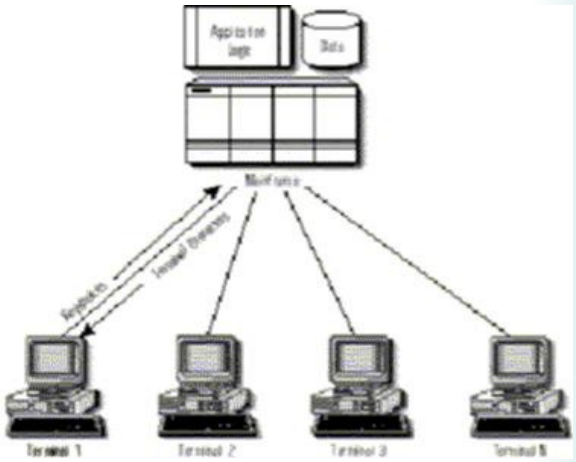
“We are currently under attack from an Internet VIRUS. It has hit UC Berkeley,UC San Diego, Lawrence Livermore, Stanford, and NASA Ames. The virus comes in via SMTP, and then is able to attack all 4.3BSD and SUN (3.X?) machines. Itsends a RCPT TO that requests that its data be piped through a shell. It copies in a program, compiles and executes it. This program copies in VAX and SUNbinaries that try to replicate the virus via connections to TELNETD, FTPD,FINGERD, RSHD, and SMTP. The programs also appear to have...”

Seguridad externa: un método

- Elabora una lista del software que necesitas
- Ejecuta **solamente** ese software
- Incluye su home page en la lista
- Revisa semanalmente las páginas de la lista

Virus, troyanos, gusanos, bichos

- Nadie está exento
- Acciones subrepticias
- Redes de zombies
- Carrera de armas
- Políticas



¡Hey! ¡No me espíes!

- La leyenda de Bob y Alice
- ¿Encriptar? ¿Qué es eso?

Te vamos a encriptaaar..

¡MUAHAHAHAAAA!!

¡Hey! ¡No me espíes!

- La leyenda de Bob y Alice
- ¿Cifrado? ¿Qué es eso?
- El cifrado es seguro. **Si lo usas bien**.

#emailselfdense

https://emailselfdefense.fsf.org/es

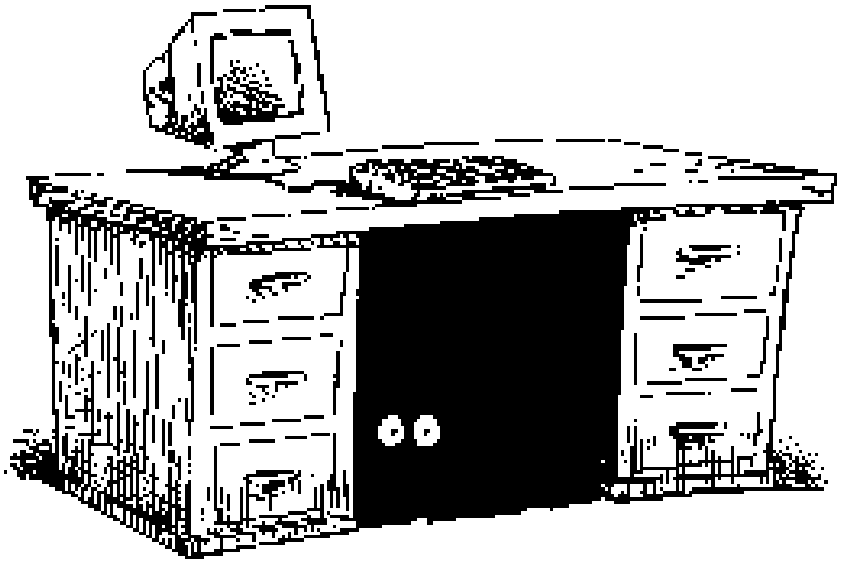
https://emailselfdefense.fsf.org/es/infographic.html

PGP

GPG

Seguridad Interna

- Frecuentemente es ignorada
- Los datos son importantes. ¿Para qué quieres a un “cracker”?
- Las computadoras son máquinas. Se descomponen.
- El factor humano.



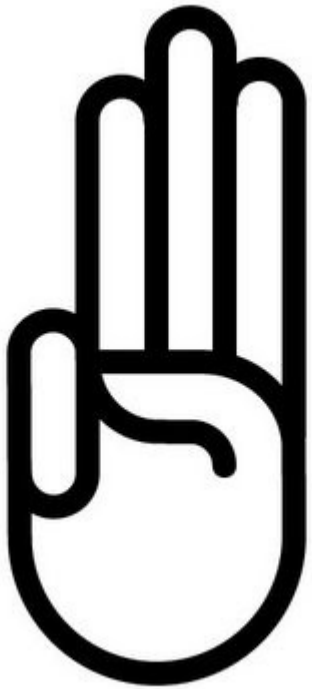
Ingeniería social

- Ejemplo – Consultores
- Ejemplo – Kevin Mitnick
- Identificaciones
- Políticas de seguridad

Phishing

- El finado señor Kwame Ujbundi
- Bancos actualizando sus sistemas
- Contraseñas de hotmail ¡Baratas!

Los 3 pasos para dummies



- Actualízate -- legalízate
- Administra tus contraseñas
- Solo di **no** (¡La primera ***siempre*** es gratis!)

¿Administrar contraseñas?

- **NO REUTILICES** contraseñas
- Usar buenas contraseñas

aIb30&+jk

ch1ng0n&

aspen caballo paleta alma

Contraseñas – Teoría de información

Símbolo	Cantidad	Bits
Letras	26	4 y medio (bueno, 5)
Numeros	10	Aprox. 3
Símbolos	~ 8	3
Mayusculas / Minúsculas	2	1
Palabras del diccionario	30000 - 70000	~ 14-16
Sustituciones comunes: a-4, e-3, i-1, o-0, s-5	5	2-3

Contraseñas

Palabras comunes con sustituciones:

Ch1ng0n& ~ 20 bits

Aleatoria, letras, números, símbolos + mayúsculas:

aIb30&+jk ~ 63 bits

4 palabras comunes al azar:

aspen caballo paleta alma ~ 64 bits

5 palabras comunes al azar:

aspen caballo paleta alma lazo ~ 80 bits

Contraseñas

Conclusión:

Usa una frase larga y fácil de recordar.

Para máxima seguridad, usa una frase larga y con palabras significativas al azar.

Correct horse battery staple
(https://www.xkcd.com/936/)

Diceware

https://en.wikipedia.org/wiki/Diceware

2FA – Autenticación de dos factores

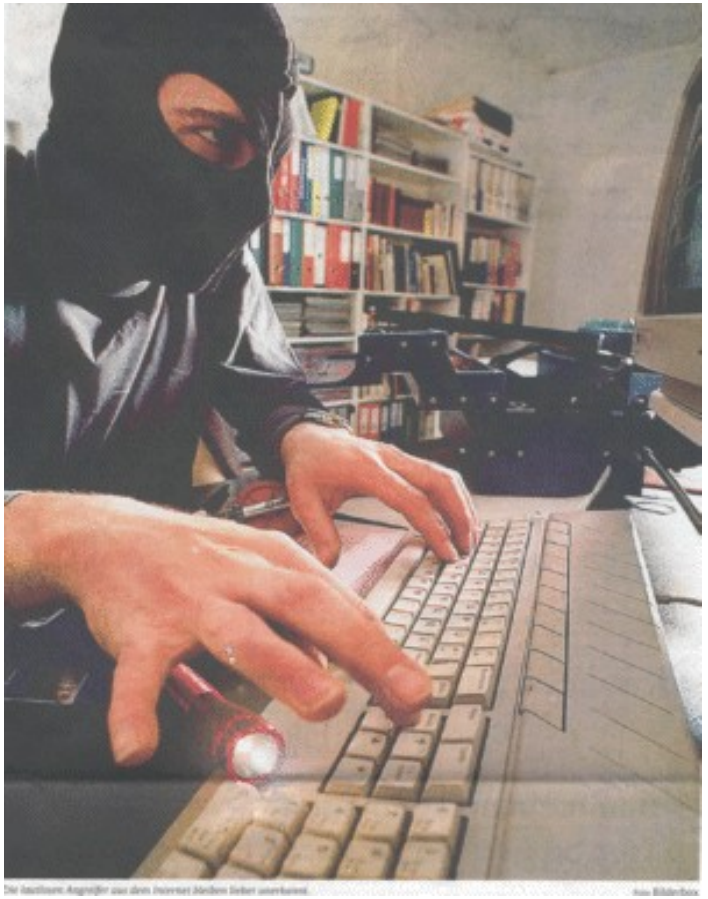
¿Quién soy?

- Algo que sé
- Algo que tengo
- NO CONFÍES EN SMS

Tu correo electrónico es la llave maestra

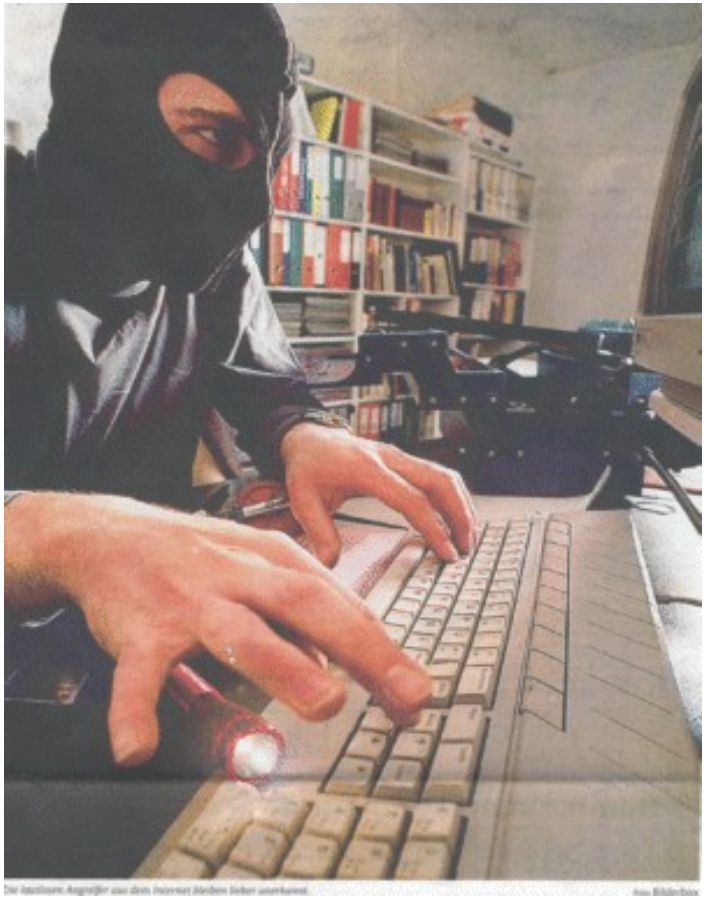
“Te vamos a mandar un código de recuperación...”

Seguridad física



- El ambiente
- Control de acceso
- Crackers en la consola
- Contraseñas y sistemas de validación

Seguridad física



Medios de arranque:

- USB
- CD
- init=/bin/bash

Respaldos

- Medios de respaldo
- Un plan de respaldo
  - Respaldo total
  - Respaldo incremental
- Respaldos fuera del sitio
- Cuando el desastre llega...

Respaldos

- tar
- rsync
- deltacopy
- backuppc

Cuida tus datos, cuida tu info

Debo respaldar mi información...

Debo respaldar mi información...

Debo respaldar mi información...

Debo respaldar mi información...

Debo respaldar mi información...

Debo respaldar mi información...

Debo respaldar mi información...

Contacto / Mas info

Felipe Eduardo Sánchez Díaz Durán
izto@izto.org

asic-linux.com.mx