



LabCAD
LABORATORIO COMPUTACIONAL DE APOYO A LA DOCENCIA

SEGURIDAD Y PRESENCIA DIGITAL

Luis Joel Donato Jiménez
LabCAD- UPRRP

BOSQUEJO

- Copias de resguardo
- Protegiendo sus dispositivos
- Protegiendo su presencia en la red
- Administradores y generadores de contraseña

COPIAS DE RESGUARDO (BACKUPS)

- Primera y más importante línea de defensa y protección de nuestra vida digital
- Todos reconocen su importancia, muy pocos son consecuentes.
- Es muy fácil (...no hay excusa).



TIPOS DE RESGUARDO

- **Manuales**

- Difíciles de mantener

- **Automáticos**

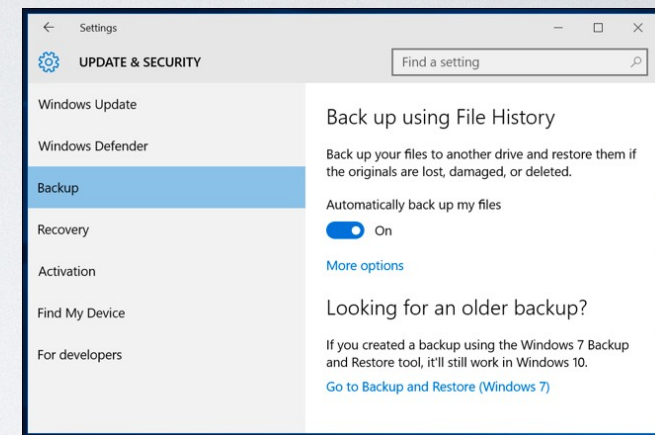
- Copias exactas de partes o del todo
- Copias exactas con capacidad de arranque (bootable)
- Incremento
 - Por versión o sólo últimos cambios

- **Nube (manuales o automáticas)**

- Más lentas y limitadas en espacio, pero a veces más convenientes

ESTRATEGIAS DE RESGUARDO

- Mantenga las copias actualizadas, al día.
- Mantenga más de una copia, en localidades distintas.
 - Resguardo contra fuego, robo, inundación, daño...



- Mac- Time Machine (todo). Otros- Carbon Copy Cloner, Super Duper
- Windows- Backup File History (solo algunos folders). Otros programas (Acronis, ShadowProtect)

PROTEGIENDO SUS DISPOSITIVOS

- Active contraseña de acceso para sus dispositivos electrónicos: computadora, teléfono, tableta...
- Active contraseña de activación luego de un periodo de “sleep” o “hybernate”
- Si tiene material confidencial, considere “encriptar” o esconder dichos documentos.
- Asegure físicamente sus dispositivos con candados
- No deje bultos visibles en el auto, no deje bultos desatendidos en su oficina o pasillos. No deje equipos bajo el sol.

PROTEGIENDO SUS DISPOSITIVOS

- Si su sistema lo permite, utilizar mecanismos de borrado y/o bloqueo remoto (remote wipe, remote lock).
- Considerar programados de localización remota (Find my (Mac, iPhone, iPad, Windows,), preyproject.com (\$), Google Maps (Android), proveedor celular (\$, ATT, T-Mobile)...))
- Mantener su sistema y programados actualizados/al día. (incluyendo Antivirus)

PROTEGIENDO SU PRESENCIA EN LA RED

- Cada vez pasamos más horas “conectados”.
- Desarrollamos una o múltiples “personas”
- Compramos más.
- “Compartimos” más información personal, familiar y laboral.
- ¿No tenemos nada que esconder?



PRESENCIA EN LA RED- ¿QUÉ PROTEGER?

- Información de contacto (dirección, número de teléfono)
- Localización
- Información financiera
- Datos personales (edad, lugar de nacimiento, padres)
- Información médica
- Historial de compras
- Historial de lugares que visitamos en la red
- Historial de email
- Entre otras...

“El que sea paranoica no elimina el hecho de que realmente me estén persiguiendo.”



?

MUCHO MÁS QUE HACKERS (¿A QUIÉN LE IMPORTA...?)

- **Hackers** (los malos)
- “Corredores de información” (**Data Brokers**)- recopilan datos y crean perfiles
- **Google, Facebook, Amazon, Twitter**, etc.
- **Gobiernos**- tanto locales como foráneos
- **Publicidad**- Internet gratis, lo barato puede salir caro. Cookies entre sitios
- Instituciones **financieras**
- Dueños de **derechos** (de autor, media)
- **Amigos** (y no tan)- parejas (presentes, pasadas y “futuras”), amigos que les gusta el chisme, patronos, compañeros de trabajo, vecinos, criminales cercanos
- Creadores intencionales de **daño**- “doxxers”, invento de crimen, revelación de info privada

PRESENCIA EN LA RED- CASO I- MAT HONAN

- **Amazon da acceso a los hackers**

- Se hacen pasar por Honan, llaman, con username, email y dirección de cobro y Amazon le permite entrar “nueva” tarjeta (número de tarjeta inexistente pero con los parámetros reales)
- Luego llaman que no pueden recuperar el password. Amazon pide nombre, dirección y número de tarjeta (la falsa). Entonces cambian password y acceden para ver los últimos números de la tarjeta de crédito real.
- Con esos datos reales, Apple les da acceso a la cuenta **iCloud**, que a su vez les dio acceso a **Gmail** (mismo email de recuperación). En estos dos sitios, se cambió la contraseña, impidiendo el acceso del dueño original. También se cambió la cuenta de **Twitter** (mismo email)
- Resultado- Cuenta de Google borrada. Twitter suspendido por comentarios racistas y homofóbicos. iPhone borrado. Computadora borrada (SIN BACKUP!!). Decenas de horas perdidas. Pudo ser peor: los hackers sólo querían fastidiar con su username de Twitter, no robaron su dinero, ni involucraron a otros.

PRESENCIA EN LA RED- CASO 2- HEARTBLEED

- Heartbleed fue un “bug” en el código de OpenSSL (<https>, entre otros)
- Permitía, hasta principios de abril de 2014, tener acceso a nombres de usuario y contraseñas de lugares que usan OpenSSL (cerca de 500,000)
- Lugares que sugieren u obligan el cambio de contraseñas: Google, Yahoo, Facebook, Instagram, Pinterest, Tumblr, Amazon Web Services, Flickr, Netflix, SoundCloud, YouTube, Dropbox, GitHub, Wikipedia, Wordpress, entre otros tantos.

PROBLEMAS DE SEGURIDAD EN 2021

- Año record
- A 30 de septiembre- 1,862 “breaches”
- Sectores más afectados-
 - Manufactura y Utilidades- 48,294,629
 - Médico- 7,000,000 +
 - Banca y Finanzas- 1,600,000
 - Servicios profesionales- 1,500,000
 - Gobierno- 1,400,000

PROBLEMAS DE SEGURIDAD EN 2021

- Datos de usuarios de aparatos **Androide**- 100 millones
- Datos de Visitantes a **Tailandia**- 106 millones
- Aplicación **Raychat (mensajería)**- 150 millones
- Portal **Stripchat (portal mensajería vídeo “adulto”)**- 200 millones
- **SocialArks** (con info de redes sociales como **Facebook, IG y LinkedIn**)- 214 millones
- Datos financieros de **brasileños**- 223 millones
- **Bykea** (Pakistán, movilidad/tránsito y entrega de paquetes)- 400 millones
- **Facebook**- 553 millones
- **LinkedIn** - 700 millones
- **Cognyte** (firma de ciberseguridad)- 5 mil millones
- **Otros** ataques- Ubiquiti, Clubhouse, USCellular, Robinhood, Twitch, T-Mobile, Panasonic, GoDaddy, Verkada, Rapid7, DreamHost, Colonial Pipeline

Henriquez, M. (2021). The top data breaches of 2021. Security Magazine. <https://www.securitymagazine.com/articles/96667-the-top-data-breaches-of-2021>
<https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/>

PRESENCIA EN LA RED- ¿QUÉ NO HACER?

- Usar la misma contraseña en todo sitio
 - Una vez descubierta, se tiene acceso a toda nuestra información
- Darle poca importancia a su correo electrónico
 - Si alguien logra acceso, procede a pedir “password reset” en todos los lugares y secuestra las cuentas
- Contestar de forma veraz las “preguntas de seguridad”
 - Muy fácil conocer información personal
- Tener una “libretita de contraseñas” (o doc de Word, Google Docs...)

PRESENCIA EN LA RED- ¿QUÉ NO HACER?

- Contestar o activar todo enlace en los emails
 - ¿realmente su cuenta del Chase o PayPal fue comprometida? Vaya al sitio directamente.
- Confiar ciegamente en Google, Facebook, o cualquier otra compañía cuyo negocio principal sea la recolección y manejo de sus datos personales y vida “online”
- Oprimir “Me gusta” indiscriminadamente. Aceptar “Amigos” que no lo son.
- Hacer cuentas nuevas porque se nos olvidó la contraseña (especialmente el Apple ID)
- Y, claro, compartir información personal en las redes indiscriminadamente.

PRESENCIA EN LA RED- ¿QUÉ HACER? ALTERNATIVAS

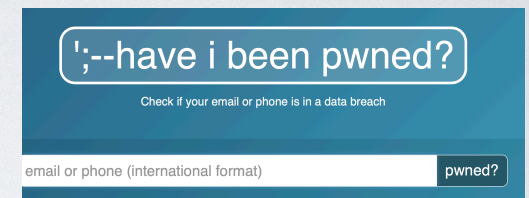
- Usar contraseñas difíciles de adivinar (“strong passwords”)
 - Combinaciones de caracteres.
- Utilizar múltiple envío de “password reset”, si el portal lo provee
 - Si alguien procede a pedir “password reset”, usted recibirá notificación a su celular u otro dispositivo, y sabrá que fue comprometido.
- Contestar lo mismo en cada “pregunta de seguridad”, o algo sin sentido
 - Debe recordar lo contestado

PRESENCIA EN LA RED- ¿QUÉ HACER? ALTERNATIVAS


- Utilizar “**Two-factor (two-step) verification o authentication**”
 - Este es un proceso que obliga, para poder entrar a cualquier servicio que lo provea, a proveer dos códigos, uno de conocimiento (contraseña) y otro de posesión (ej, teléfono)
 - Al entrar la contraseña, el sistema le envía al teléfono un código corto, que deberá ser entrado en ese preciso instante. De esta forma, el hacker no puede entrar a su cuenta si a su vez no posee el teléfono de la víctima.

PRESENCIA EN LA RED- ¿QUÉ HACER? ALTERNATIVAS

- Tratar de descubrir su información en la red
 - “Go hack yourself”- search, **Have I been pwned?**
- Leer las políticas de privacidad de los lugares que frecuenta.
- Usar programas de email que permitan bloquear contenido remoto.
- Hacer inventario de sus activos digitales.
- Si lo entiende necesario, preparar documento para su abogado/a con la información necesaria para que ésta, usted o una persona cercana pueda recuperar sus datos, especialmente si usted falta o está incapacitado.



PRESENCIA EN LA RED- ¿QUÉ HACER? ALTERNATIVAS

- Asegurar su conexión a la red
 - Navegar en **privado** (private, incognito)
 - Tratar de siempre estar conectado con websites que usen SSL (**https**, candado) 
 - Programas de monitoreo de red (**Little Snitch, ZoneAlarm**)
 - Virtual Private Network (**VPN**), especialmente en WiFis públicos
 - Si usa WiFi, que su contraseña sea **WPA** (WPA2 o WPA3)
 - Para situaciones extremas- no usar Google como buscador (**DuckDuckGo**)

PRESENCIA EN LA RED- RETO

- Cada vez más, activamos cuentas en diferentes portales en la red.
- Los requisitos de seguridad de las cuentas varían y cada vez son más estrictos (nuevas combinaciones de caracteres en las contraseñas)
- Las “preguntas de seguridad” son cada vez más imprecisas y no necesariamente poseen contestación clara o única
- Cada vez es más difícil mantener inventario de tanto nombre de usuario y tanta contraseña

PRESENCIA EN LA RED- RETO

- ¿Cómo recordar tanta contraseña?



ADMINISTRADORES DE CONTRASEÑAS

- Existen múltiples programas que permiten manejar, archivar, generar y recuperar contraseñas
- Estos programas proveen un lugar “seguro” dónde guardar su información confidencial, mientras usted sólo necesita recordar una contraseña maestra.



Muchas gracias

Sesión de preguntas y comentarios

luis.donato3@upr.edu

LabCAD
LABORATORIO COMPUTACIONAL DE APOYO A LA DOCENCIA