MANEJO "MENOS INSEGURO" DE LAS REDES SOCIALES – PREVINIENDO DELITOS

F4Lc0N – LowNoise Hacking Group

"La tecnología no es una panacea". Esta es una de las leyes inmutables de la seguridad informática (y aplica a cualquier tipo de seguridad) … No todos los problemas pueden ser solucionados con tecnología, y mucho menos los que son causados directamente por la tecnología.

Lamentablemente (y a la vez afortunadamente) nacimos y/o crecimos en un país del tercer mundo, con todos sus problemas y delicias, y dentro de estas consecuencias automáticas tenemos:

- Poco acercamiento a la tecnología durante nuestros primeros años de educación (ya siendo esto mejorado, de forma mínima)
- Poco acceso a la tecnología , si no se tienen los recursos económicos suficientes
- Cuando hay contacto con la tecnología de punta, nuestra recursividad innata nos ayuda a identificar la mejor forma de "emplearla para nuestro beneficio", y no de "emplearla DE FORMA SEGURA", para nuestro beneficio
- Tenemos el gen de "chicanear", un poco más desarrollado que el de mantener un entorno seguro, por dentro, a nuestro alrededor inmediato, y alrededor de nuestros seres queridos

Estos factores me han permitido durante los últimos 15+ años evaluar de manera ingeniosa (hacking) la seguridad de diversos elementos y de su uso cotidiano (teléfonos fijos, teléfonos celulares, redes de datos, bandas magnéticas, bluetooth, infrarrojo, tarjetas de proximidad, comunicaciones satelitales, sistemas de televisión, sistemas de control industrial, en fin ….), y todo eso gracias a esa malicia que sólo puede ser desarrollada a través de la recursividad necesaria para superar los obstáculos que día a día se pueden presentar en este hermoso tercer mundo …

Esta malicia o ingenio lo tenemos todos los que vivimos acá, y cada día lo desarrollamos más. Lamentablemente esto aplica no sólo a la gente de bien, sino también a los delincuentes (informáticos y del mundo físico). Ellos también están "en la jugada", aprendiendo cada nuevo truco, cada nueva ventaja que la tecnología puede brindar a su modo de vivir …

Con el surgimiento de las redes sociales (principalmente enfocándonos en Facebook y Twitter), hemos tenido un nuevo despertar en lo que significa hoy en día "estar conectados", permitiéndonos compartir información en tiempo real, enterándonos de noticias (i.e. muerte de Bin Laden, terremoto+tsunami en Japón, etc.) mucho antes que a través de las noticias, compartiendo trabajo y conocimientos con gente afín al otro lado del mundo, en instantes, etc.

Para los que vivimos de la tecnología, por la tecnología y/o para la tecnología, estas herramientas son muy valiosas. Para las personas que no dependen directamente de la tecnología en su vida diaria (cada vez menos), también pueden ser útiles, permitiendo un contacto más directo con

personas que están lejos, o con las que no tenían contacto hacía un tiempo (excompañeros de colegio, universidad, etc.). En fin, cada día hay nuevos e ilimitados usos para estas redes sociales.

Sea la razón por la que las usamos, o el uso que le damos, no siempre seguimos unas mejores prácticas de seguridad, que nos permitan prevenir y/o detener un delito/crimen. A veces simplemente al usar estas tecnologías de forma indebida, estamos "dando papaya".

Es por esto que decidí escribir este documento, con ayuda y tips de Eduardo Chavarro (Twitter: @EChavarro), para listar una serie de recomendaciones de uso seguro de estas redes sociales, que nos permitan mantener un entorno menos expuesto:

- **OPERACIONES FINANCIERAS:**
    - Nunca publique información sobre sus retiros, ingresos o pagos
      (i.e. "Hoy me deben consignar esa platica … Apenas entre te aviso por acá", "Ehhh, pagaron la quincena !!!", etc.)
    - Nunca publique información sobre el/los sitio(s) y/o horarios en que realizará operaciones financieras
      (i.e. "Alguien sabe a qué hora cierra el Banco X de la Calle 72 con 15 esta noche ?", "El Banco Y como siempre con su portal caído … Me tocó ir a retirar esa plata al cajero de la esquina", etc.)
    - En lo posible, ni siquiera mencione las entidades financieras en donde tiene sus cuentas
      (i.e. "Ya tengo cuenta de ahorros en Banco X !!!", "Estoy cansado del pésimo servicio en Banco Y", etc.)
    - Mucho menos envíe información privada (como sus números de cuenta, claves, etc.) por estos medios. Si es estrictamente necesario (por urgencia o algo así) use Mensajes Directos (DMs), aunque igual, no son 100% privados. Es mejor enviar esa información segmentada, por varios medios (SMS, email, llamada telefónica, etc.)
      (i.e. "Consígname por favor en mi cuenta aaaa-bb-cc-dddd del Banco Z", "¿Amor, cambiaste la clave de la tarjeta de débito? No me funciona…")
    - Y sus combinaciones:
      @esposo (9:15am): "Me encanta como combinan esa faldita azul con esa blusa rosada, en ti"
      @esposa (5:25pm): "Amor, ya me consignaron el préstamo de los $40M, pero tú cambiaste la clave de la tarjeta débito ? '1234' ya no me funciona. Estoy en Banco X de la Cra 11 x 95."
      @esposo (5:31pm): "La cambie por seguridad, ahora es '0123'. Retira por ventanilla mejor, unos $5M, y te espero en el apto"
      @esposa (5:33pm): "OK, Ya me está ayudando un Sr. en el cajero. También le gustó mi blusita rosada ;)"
      @esposa (5:33pm): "Afuera hay taxis esperando, ya te aviso cuando tenga la $ y salgo para allá …"

- **TAXIS – PASEO MILLONARIO:**
  - En lo posible, nunca tome un taxi en la calle, y menos de los que están parqueados esperando a la salida de centros comerciales, bancos, etc., a menos que sean operados directamente por la empresa de taxis.
  - Apenas ingrese a un taxi, siempre coloque los seguros de las puertas traseras, y manténgase alerta de cualquier comportamiento extraño del conductor, y/o de personas o carros a su alrededor.
  - Si desea publicar/twitear la placa del taxi en que va, recuerde que la placa puede ser falsa y solo es desatornillarla para cambiarla. Publique mejor la placa y el # de móvil (un poquito más difícil de cambiar).
  - Nunca publique su ruta y/o destino
    (i.e. "Ya voy en camino, nos vemos al frente del Restaurante X del Centro Comercial Y", "Toda la Av. Quito estaba trancada, ya acá en la 92 está fluyendo …")
  - Si va a publicar información IMPORTANTE desde el taxi (como la placa y # de móvil), hágalo rápidamente brevemente. No "dé papaya" distrayéndose en su celular.
    (i.e. "Voy en un taxi amarillo de placa BBB-123, por la carrera séptima con 45" → "Huy, hay trancón, y va a llover…" → "Bueno, será jugar Angry Birds hasta mi destino en la Cra 1 # 2-3")
  - Recuerde que para un delincuente haciéndose pasar por taxista, es mucho más interesante una víctima que está "hipnotizado" dentro de un celular (usualmente de gama alta), antes o después de recogerlo, que un pasajero que está atento a todo a su alrededor, de la ruta, del tráfico, etc.
  - En lo posible trate de pedir el taxi por teléfono o celular, pidiendo la confirmación de la placa y del número de móvil. Sólo aborde el taxi que tenga los datos exactamente como se los confirmaron por teléfono, y envíe su tweet o mensaje con los datos del taxi ANTES de que este llegue.
  - Y su combinación:
    @esposa (3:27pm): "De compras en C.C. Fifilandia $$$:D http://4sq.com/kzmjtk"
    @esposa (5:33pm): "Alguien sabe cómo pido un taxi por Twitter ? :P"
    @esposo (5:40pm): "Llama al 031-9999999 y pídelo desde tu cel … Apúrale que ya estoy en la casa ! :) http://4sq.com/gyujtk"
    NOTA: Gracias a FourSquare, el atacante ya tiene origen y destino del taxi
    @esposa (5:45pm): "Esto está tenaz, todos los taxis están llenos … y yo con todas estas bolsas :("
    @esposa (5:49pm): "#QueSuerte ! Venía un taxi solito, no recogía a nadie y paró a recogerme a mí … más lindo !!! :D ;) :P"
    @esposa (6:06pm): "Amor, ya estamos cogiendo la Av. Circunvalar acá en la Calle 94, llego en 10 mins !!!"

@esposa (6:15pm): “Hmm, me estoy quedando sin batería, será por jugar tanto Rayman, o será q por esta ruta nueva que tomó el taxista no hay buena señal y eso me come batería?”

- **Y OTRAS – DE SENTIDO COMÚN:**
  - Nunca informe cuando su casa, oficina, etc. se van a quedar solas
    (i.e. “Ya acabé este informe !!! Me voy, esto parece embrujado de lo sólo …”, “@vecina échemele un ojito a la casa que queda sola”)
  - Nunca avise cuando sale de su casa por períodos prolongados
    (i.e. “Que rico estar con TODA la familia acá en la playa !”, “Miércoles, yo ya en Cartagena, y no me acuerdo si al fin dejé las luces encendidas ?”)
  - Recuerde que TODA la información en las redes sociales debe ser considerada como PÚBLICA !!! Si desea compartir información personal, utilice otros medios, o segmentación …
  - Use los mecanismos de geolocalización (Foursquare.com / Google Latitude / etc.) inteligentemente, no “dé papaya” (a los delincuentes, y en general, a todo el que no necesita conocer sus cosas privadas)
    @esposo (6:25pm): “@esposa Nada que salgo del trabajo amorcito, creo que esta noche me toca trasnochar acá … :~(“
    @esposo (9:45pm): “Con @amante en la Hab. 333 en el ‘Motel Rocksea’ http://4sq.com/klHFmT”
    @esposa (9:46pm): “Dónde es que está el bate de béisbol ?”
    @esposa (9:46pm): “Alguien sabe cómo llegar rápido a http://4sq.com/klHFmT, sin hacer mucho ruido ?”

Igual, nunca sobra ejercer un poquito el sentido común en estos mundos virtuales. Aquí unas recomendaciones generales para tener siempre en cuenta:

- Lo expuesto anteriormente también aplica a otras redes sociales, a mensajes de texto de celular (SMS/MMS), publicación de fotos en Internet, mensajes de PIN de Blackberry, etc.
- No “sufra” por no estar twitteando/publicando … Nadie se va a morir, ni Ud. Va a dejar de ser “cool”, por que no haya un tweet/post suyo durante 30 minutos.
- Siga recomendaciones básicas de protección que constantemente envían las mismas redes sociales. Justamente hoy me llegó este interesante link de Facebook: https://www.facebook.com/notes/facebook-security/keeping-you-safe-from-scams-and-spam/10150174826745766 (Léelo !!!)
- Otras fuentes de concientización, para uno mismo y para compartir con los que lo rodean, son importantes. Ver por ejemplo: http://pleaserobme.com/
- Siga buenas prácticas de seguridad en TODAS las áreas (no sólo en redes sociales). Recuerde que un ataque específico contra Ud. Seguramente sumará fuerzas en diferentes

ámbitos: Use contraseñas fuertes, no comparta su PC, utilice prevención de malware (antivirus, antispyware, etc.), no abra correos/URLs extrañas, etc.

DISCLAIMERS:

- Algunos mensajes sobrepasan los 140 caracteres (límite de Twitter) sólo para dejar el punto claro
- Toda la información expuesta en este documento es el resultado de experiencias propias y recolectadas, durante años, y este conocimiento no ha sido utilizado de forma ilegal por el autor, en ninguna manera
- La información expuesta se libera únicamente de forma informativa y educativa. Cualquier uso ilegal de ésta es responsabilidad única del lector, quien expresamente libera al autor de toda responsabilidad
- Este documento se libera bajo la Licencia "**Creative Commons Attribution-NonCommercial-ShareAlike** (**CC BY-NC-SA)**"

Resumen: "Esta licencia permite a otros mezclar, modificar, y construir sobre el trabajo licenciado, de forma no comercial, mientras se dé crédito al autor, y las nuevas creaciones se licencien bajo los mismo términos."

Mayor Información

F4Lc0N – LowNoiseHG – Colombia

Twitter: @falcon_lownoise

Email: falcon@lownoisehg.org

URL: http://www.lownoisehg.org/