REDES SOCIALES

SEGURIDAD

Autor: Roberto Guillermo Berenguel Vinck

REDES SOCIALES Y SEGURIDAD

- Qué es una red social y cuáles son las más comunes
- Amenazas más comunes en la red
- Ataques de ingeniería social y hacking
- Caso de Facebook
- Esclavos del algoritmo - Elecciones
- Conclusiones

Autor: Roberto Guillermo Berenguel Vinck

QUÉ ES UNA RED SOCIAL

Las **redes sociales** son sitios de Internet formados por comunidades de individuos con intereses o actividades en común (como amistad, parentesco, trabajo) y que permiten el contacto entre estos, de manera que se puedan comunicar e intercambiar información.

Los individuos no necesariamente se tienen que conocer previo a tomar contacto a través de una red social, sino que pueden hacerlo a través de ella, y ese es uno de los mayores beneficios de las comunidades virtuales.

El **origen de las redes sociales** es bastante reciente, se puede decir que surgen en 1995 con la creación de classmates.com, a manos del estadounidense Randy Conrads. Esta red social buscaba reunir ex compañeros de colegio, o universidades.

Fuente: http://concepto.de/redes-sociales/#ixzz5H6dxURqZ

Autor: Roberto Guillermo Berenguel Vinck

UNJUPRAC
Delegación Puebla

REDES SOCIALES MÁS COMUNES

Tipos de redes Sociales
Si se quisiera clasificar a las redes sociales, podría hacerse según su origen y función:

Redes genéricas: Son muy numerosas y populares (como Facebook o Twitter).
Redes profesionales o negocios: Como LinkedIn, que involucran individuos que comparten el ámbito laboral o que buscan ampliar sus fronteras laborales y pueden ser abiertas o cerradas.
Redes temáticas: Relacionan personas con intereses específicos en común, como música, hobbies, deportes, etc., siendo la más famosa Flickr (temática: fotografía).

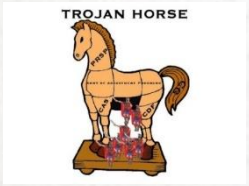
Fuente: http://concepto.de/redes-sociales/#ixzz5H6tkpvxZ

Autor: Roberto Guillermo Berenguel Vinck

AMENAZAS MÁS COMUNES EN LA RED

VIRUS: Cualquier programa (o código) capaz de autoreplicarse con la intervención del usuario.

Gusano.- Tiene la propiedad de duplicarse a sí mismo, residen en memoria y se duplican a sí mismo. Los gusanos no dañan archivos pero sí repercuten el funcionamiento de la red. **NO necesitan la intervención del usuario.** Su objetivo es colapsar computadoras y las redes en que están conectados impidiendo trabajar a los usuarios. No infecta archivos.



Troyano.- Es un programa en el que código malicioso o dañino es ejecutado sin el conocimiento del usuario. Viene acompañado de un programa "inofensivo" y tiende a abrir puertos de comunicaciones, instalar "keyloger|s" y/o robar claves de acceso. No es un virus.

Malware.- ("malicious software") cualquier programa o ficha desarrollado con el propósito de hacer daño. Malware incluye virus, troyanos y gusanos entre otros.

Fte: varios Internet

Autor: Roberto Guillermo Berenguel Vinck

AMENAZAS MÁS COMUNES EN LA RED

Spyware.- Tecnología que ayuda en la captura de información sin el conocimiento del usuario.

Adware.- Programa que lanza publicidad indiscriminadamente interrumpiendo al usuario.

Phishing.- Técnica usada para extraer información confidencial mediante la ingeniería social o engaño.

Fte: varios Internet

Autor: Roberto Guillermo Berenguel Vinck

ATAQUES DE INGENIERÍA SOCIAL Y HACKING

Ingeniería Social. - es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

- La ingeniería Social está definida como un ataque basado en engañar a un usuario o administrador de un sitio en la internet, para poder ver la información que ellos quieren.
- Se hace para obtener acceso a sistemas o información útil.
- Los objetivos de la ingeniería social son fraude, intrusión de una red.

La ingeniería social **se basa en cuatro principios básicos** que aprovechan la confianza de los usuarios:
Todos queremos ayudar. El ejemplo más sencillo serían los correos de cadena.
El primer movimiento es siempre de confianza hacia el otro, aunque es cierto que la gente suele desconfiar más en Internet. Para ello, se cambian los remitentes para que resulten de confianza para los usuarios, como un paquete para recoger en correos, una notificación para ver el estado de la declaración de hacienda, etc.
No nos gusta decir No, de manera que, en lugar de no ejecutar la aplicación que nos va a mostrar cómo está nuestra devolución de la renta, por ejemplo, acabamos por hacerlo, poniendo en riesgo la seguridad de los sistemas informáticos de nuestra empresa u hogar.
A todos nos gusta que nos alaben, lo que al final logra crear simpatía para revelar información confidencial.

Fte: varios Internet

Autor: Roberto Guillermo Berenguel Vinck

ATAQUES DE INGENIERÍA SOCIAL Y HACKING

Ejemplos:

- Phishing. Ya comentado anteriormente
- Baiting. Se **abandonan dispositivos como memorias USB** con la intención de que alguien las encuentre y conecte a sus equipos. Es en ese momento cuando se produce la infección. De esta forma se propagó el **virus Stutnex** en las centrales nucleares de Irán, para entorpecer el programa de enriquecimiento de uranio.
- Es el caso de la estafa del **príncipe nigeriano**,

Hacking.- es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

Ejemplo: Hacking ético. Es la ciencia que trata sobre el uso de técnicas de ataque para encontrar fallas de seguridad en los sistemas de información, con el permiso de sus propietarios, con el único objetivo de mejorar la seguridad.

Fte: varios Internet

Autor: Roberto Guillermo Berenguel Vinck

CASO DE FACEBOOK

En marzo de 2018, medios liderados por The Guardian, The Observer y The New York Times revelan que Cambridge Analytica influyo en las elecciones de 2016, en Estados Unidos. Para ello utilizó información de millones de usuarios de Facebook: Esto fue lo que ocurrió, según investigaciones periodísticas:

1	2	3	4	5	6
Facebook permite que Aleksandr Kogan, profesor de la Univ. De Cambridge, recabe datos de sus usuarios. Kogan usa la app thisisyourdigitallife Los usuarios autorizan el acceso a su ubicación, amigos y a todos sus "likes"	El profesor entrega esos datos a Cambridge Analytica (CA), con lo que supuestamente viola las reglas de Facebook. Son más de 50 millones de perfiles. CA es contratada por el equipo de campaña de Donald Trump en 2016	Facebook insiste en que no hubo violación de datos, porque permite que investigadores tengan acceso a su información para fines académicos (los usuarios dan su consentimiento al abrir una cuenta, asegura)	Cuando Alexandre Nix, ex CEO de CA, es líder de SCL Group, se obtienen datos en Caribe y África, donde sus reglas de privacidad son laxas. En 2013 prueban mensajes psicográficos en las elecciones a gobernador en Virginia.	En 2014, Cambridge Analytica moviliza contratistas y empleados de SCL Group en todo Estados Unidos, debido a las elecciones legislativas.	En las elecciones presidenciales de 2016, CA dirige anuncios digitales que modelan la participación del electorado y paga 5 millones de dólares en anuncios de TV.

Fte: revista Tec Review mayo/junio 2018

Autor: Roberto Guillermo Berenguel Vinck

ESCLAVOS DEL ALGORITMO - ELECCIONES

“En la noche del 1 de octubre de 2017, Stephen Paddock disparó desde el piso 32 de un hotel en las Vegas y, en menos de 15 minutos, mató a 58 personas y dejo heridas a 851. Es el mayor asesinato en masa cometido por un individuo en Estados Unidos. Cuando a la mañana siguiente, los ciudadanos quisieron consultar la noticia en Google, se toparon con varios blogs que describían a Paddock como simpatizante liberal y anti-Trump. Además aseguraban que el FBI había revelado su conexión con ISIS y que los medios querían ocultar que se había convertido al islam. ” TODO lo consultado, a excepción de la masacre, ERA FALSO.

La estrategia tenía un motivo político: apuntalar la popularidad de Trump y fomentar el miedo entre la población a los ataques terroristas.

“Esto incidentes son el resultado de esfuerzos intencionales para manipular los algoritmos de búsqueda y dirigir al usuario hacia un contenido en particular”, advierten Dipayan Ghosh y Ben Scott, autores del reciente estudio Digital Deceit.

Aunque parezca sorprendente, la desinformación es legal. Está protegida por la libertad de expresión; por lo que es difícil de frenar

Fte: revista Tec Review mayo/junio 2018

Autor: Roberto Guillermo Berenguel Vinck

ESCLAVOS DEL ALGORITMO - ELECCIONES

Se estima que, por cada individuo de Estados Unidos, hay como 5000 puntos de datos disponibles para análisis.

La desinformación digital puede calar en gran escala en la sociedad y alcanzar, incluso, a audiencia reacias a dejarse convencer, gracias a la combinación de herramientas poderosas: internet, los algoritmos y la propaganda de precisión. Es decir, el uso de inteligencia artificial (IA) para determinar perfiles de usuarios y destinatarios idóneos para las campañas y la creación de mensajes que apunten al talón de Aquiles de cada uno de ellos.. Porque "los sentimientos individuales sobre ideas o candidatos políticos suelen ser impresionables y, por lo tanto, manipulables."

¿ Qué sucede cuando se trata de vender candidatos electorales? Han desarrollado estrategias brillantes de persuasión activa. Pero también han abierto la puerta a excesos que pueden dañar el interés público y la cultura política, debilitando la integridad de la democracia.

En otras palabras, lo peor que te puede pasar es que seas manipulado en tu modo de sentir, en tu visión política … y en tu voto. Y, contigo, millones de personas más.

Fte: revista Tec Review mayo/junio 2018

Autor: Roberto Guillermo Berenguel Vinck

ESCLAVOS DEL ALGORITMO - ELECCIONES

"En redes sociales se obtiene nuestro perfil, qué pensamos de cierto temas. También se obtiene un antiperfil. Ambos determinan si pueden influir o no sobre nosotros"

Mejor que un padre!!!

Un día, un investigador de Cambridge, experto en psicometría, se le ocurrió comprobar cuanto podría saberse sobre un perfil psicológico de una persona estudiando su actividad en FaceBook. Michal Kosinski lanzo una petición pública de voluntarios para su experimento, que consistía en hacer tests de personalidad a quienes le daban acceso a su página de la red social.
En un abrir y cerrar de ojos y sin esperarlo, se encontró con millones de voluntarios. Cruzando los resultados del test psicológico y los "Me Gusta" en Facebook, creo borradores cada vez más refinados de un algoritmo de IA capaz de hacer una radiografía a la forma de ser de cada persona, solo con tener acceso a sus "likes". Con 150 "Me Gusta" el algoritmo podía perfilar la personalidad de un voluntario mejor que sus padres.

Bots (Aféresis de Robot):
Cuando se habla de esta figura, se refieren a cuentas que no pertenecen a usuarios reales: son gestionadas por un software encargado de imitar el comportamiento humano para hacerse pasar por una persona. En agosto de 2017, Trump agradeció un tuit público a una tal Mincey por haberlo felicitado por "trabajar para el pueblo americano". Con nada menos que 150,000 seguidores.

Fte: revista Tec Review mayo/junio 2018

Autor: Roberto Guillermo Berenguel Vinck

FINALMENTE:

- Hoy día no solo las redes sociales son tomadas en cuenta generar un perfil o antiperfil de las personas, sino que cualquier cosa que pueda ser digitalizada. Muchas de las cosas que veíamos en ficción cuando niños, adolecentes o jóvenes adultos, ya son un realidad hoy día. Como ejemplo, existe en Netflix, una serie denominada Black Mirror. El capítulo es el 1 de la temporada 3, “Caída en Picada” del año 2011; idea similar a lo que hace China hoy.

Autor: Roberto Guillermo Berenguel Vinck

CONCLUSIONES:

- Debemos reconocer que el mundo ha cambiado de manera formidable por la tecnología, entre otras cosas.
- Estamos obligados a tener mayor prudencia que antes, sobre todo en lo que se encuentra uno en Internet.
- Debemos verificar las fuentes de información antes de siquiera dar un “like” o reenviar un mensaje ya sea en texto, foto o video.
- Para el momento de esta presentación, no dudo que los tres contendientes a la presidencia de este país, a través de redes sociales, estén aprovechando IA para acreditar sus programas de gobierno o desacreditar a sus oponentes. En ambos casos como es difícil saber a ciencia cierta cuales son reales y cuales no. Por lo que para formarse un criterio o tomar una decisión, creo que habrá complementar con otras fuentes acreditadas que no sean solo Internet.
- Personalmente creo que mediante IA, han prostituido tanto a las redes sociales, que no son de confiar.
- Al hacer uso de cualquier red social, se aceptan los términos de estas y su privacidad. Sin embargo no conocemos cuando estas redes permiten a académicos hacer uso de estas. El riesgo es aceptar invitaciones a investigaciones de mercado o cualquier otra cosa con un tercero que te contacte en la red.
- Así como existen cosas hechas con buena intención, como Web, existen siempre sus contraparte, Dark Web.
- Tener cuidado o revisar si en sus perfiles de usuario en las redes sociales que se encuentren inscritos, poner solo lo necesario. Si por ejemplo, no requiero poner mi ubicación, o numero celular, o fecha de nacimiento, o donde trabajo, pues no ponerlo o quitarlo.

Autor: Roberto Guillermo Berenguel Vinck

UNJUPRAC

Delegación Puebla

¡¡¡ Muchas Gracias !!!

Autor: Roberto Guillermo Berenguel Vinck