HDC

Antes de empezar la clase me gustaría decirles que estoy recibiendo cada vez menos correos. No creo estar explicando mejor, pero si realmente tienen dudas, o si quieren hablar con alguien, pueden mandar correos que los contesto en poco tiempo. Estoy para ayudar.

Elicitation

Empezamos viendo un término en inglés, como muchas otras veces. Con la diferencia de que esta vez no existe una traducción literal de este término. Pero, ¿qué significa? **Elicitation se refiere a la acción del traspaso de información fluida de un punto a otro.** Es una palabra más usada en **psicología**, pero ya que estamos en ingeniería social, no podemos olvidarnos de usar todas las herramientas posibles.

"¿Y para qué vamos a usar esta herramienta? ¿Para hackear cerebros?"

Quizás no esté del todo bien que lo digamos de esa manera. Vamos a profundizar en el hecho de **ganar acceso** a un lugar donde **no tenemos privilegios**, ya sea físico o lógico. Como dijimos, **elicitation es el flujo de información**, y para hacerlo con personas usaremos preguntas indirectas y así obtener datos sobre sus datos o problemas.

"¿Y cómo me va a contar estas cosas una persona desconocida?"

Buena pregunta, Manolo. Lo importante es que uno pueda crear una **influencia positiva** en la otra persona. Queremos que ese desconocido confunda nuestra imagen con su programa de TV **preferido**, que cuando piense en nosotros sonría por **placer**. Lo vamos a lograr porque entrenaremos nuestra persona para ser un

excelente ***comunicador*** tanto en el aspecto **verbal** como el **no verbal**.

¿Dónde?

Repasemos nuestros **escenarios** en los que estaremos:

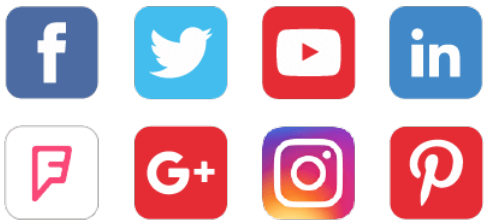
- Recepción de oficinas.
- Un bar
- Sala de esperas

Aunque en realidad, no hace falta enumerar tanto porque puedo decir que el campo morfológico de acción será siempre en un **lugar público**. Imaginen que si nos encontramos en privado es porque ya conseguimos acceso a eso con alguna técnica de ing. Social. Pero para poder tener un caso cara a cara con nuestro objetivo, podría haber sido un **encuentro pre-acordado** donde ya tenemos algo de información o nuestro primer acercamiento con un **pretexto** (veremos mas sobre pretexto en otra clase). Pasa que las maneras de obtención de información a la primera, a veces no son ideales. Si nuestro objetivo es alguien que trabaja para una empresa, podemos conseguir algo por allí, aunque lo único que podemos llegar a conseguir son nombres, contactos. Pero... No sé si alguno de ustedes puede llegar a tener **datos en Internet**, en alguna página como... no lo sé... Facebook, Twitter, LinkedIn, Pinterest, Instagram, y muchas otras **redes sociales**. Allí podemos encontrar edad, parejas, fotos, intereses, gustos, relaciones, etc.

Esto es casi absurdo. Manolo, **¿Qué pasaría si viene una persona en la calle y te pregunta datos como tu nombre, tu edad, tus gustos personales?**

“Lo mandaría a volar. Debe ser un acosador. ¿Quién se cree?”

Pero al mismo tiempo, estás compartiendo **muchísima** más **información,** de forma **masiva** con gente que ni conocés de manera **voluntaria** por redes sociales. ¿Verdad?



“Em... ¿Puedo llamar a un abogado?”

No creo. Sigamos con esto. Nosotros queremos que nuestras preguntas hagan la misma **magia** que sucedió en la historia que les conté en la primera clase. Que un simple “¿Cómo estás?” pueda escribir una página entera llena de **detalles.** Si conseguimos respuestas **monosilábicas**, es porque estamos haciendo algo **mal**. Por eso habrá **dos tipos de preguntas:**

1. Las que utilizamos para **recolectar información** que podría ser pública o de poca importancia íntima para el objetivo
2. Las que son **intrusivas** para aquella persona. Y en realidad, nuestro trabajo es que estas que son parte de un nivel de intimidad superior, pasen a la primera clasificación generando un vínculo de confianza con ella.

Otro **problema** que podemos llegar a tener es la de no poder pasar una pregunta intrusiva a una de recolección porque el **objetivo** está **consciente** de lo que significa un ataque de ingeniería social y se protege, no hablando de ciertos temas o desconfiando demasiado. Lo difícil es que **cada persona es distinta.** Tienen diferentes educaciones, culturas, límites, y nosotros tenemos que aprender a jugar con todo eso. Por eso también es muy **importante** poder **recolectar información desde Internet** u otros medios, antes, y poder saber a donde controlar una conversación.

¿Cómo?

Como dijimos anteriormente, las **preguntas** son nuestra **herramienta** para ***hostigar*** a nuestro objetivo. Entonces, queremos que sean lo más **eficientes** posibles. Para esto, tenemos que tener en cuenta la **diferencia del enfoque** de esas preguntas. Por ejemplo:

- Si usamos como pregunta "¿No le parece un desastre la atención de este lugar?" es muy posible que aunque la pregunta sea extensa, la **respuesta** pueda ser una **simple** expresión de **afirmación** como "Sí. La verdad que sí." pero no es fácil que agregue algo a su reacción.
- En cambio, si preguntamos "¿Qué le parece la atención de este lugar?" es posible que pueda comentar **un par de renglones,** y con una posible "mala. Me recuerda a la sala de espera de mi dentista." Ya podremos seguir con las preguntas y **excavar** cada vez más profundo en su intimidad.

Pero para ser un gran **elicitator** tenemos que clasificarlas en estos diferentes tipos:

1. **Final abierto**: estas son, justamente, las que recién contaba para que la persona tenga que responder con algo más que un "sí" o un "no". Que la variedad de opciones sea muy grande y esto da lugar a un relleno con detalles, a que la otra persona pueda sentir interés genuino.
2. **Final cerrado**: por ahí, en nuestro ejemplo anterior, lo vimos como el "mal ejemplo", pero lo cierto es que también puede ser útil para llevar la conversación a donde queremos. Un buen ejemplo sería "¿Hace cuántos años conoce a esta persona?" porque limita a la persona a decir un número. Puede divagar poco pero se sentirá en deuda con quien le hizo la pregunta.
3. **Preguntas neutras**: son aquellas que no importa la respuesta, siempre es correcta porque es a libre albedrío de quien la contesta. Por ejemplo "¿Qué pensás de la vida después de la muerte?" es una pregunta que no podemos juzgar, que no es retórica y también nos ayuda a que el otro se desestrese, que sienta que no es juzgado aunque sea una respuesta sin mucho sentido. Muy importantes para llegar a abrir a una persona. En general, el objetivo es aflorar un sentimiento en la otra persona y no recaudar información.
4. **Preguntas de liderazgo**: no sólo cierran a la persona en 2 respuestas posibles,

si no que también se presiona a uno de los extremos porque así vamos indicando la respuesta que queremos conseguir. Ejemplo: “¿No es cierto que hace mucho calor?”. ¿Cómo se sentirá la persona? En realidad sentirá culpa de llevarte la contra. NOTA: cuidado con el tiempo en el que se realiza esto. Si lo hacemos demasiado temprano, veremos como la otra persona siente que esa presión genera una resistencia muy grande y perderemos el control del encuentro.

5. **De suposición**: estas preguntas son bastante poderosas porque nos dan la posibilidad de desconcertar y distraer al objetivo para que nos conteste dos cosas en vez de una, o nos conteste algo simplemente por seguirnos la corriente en nuestra suposición. Ejemplo: “¿Cuál fue el mayor robo que le hiciste a la empresa?”. Ya estamos suponiendo que robó (obviamente que en este escenario no habíamos hecho esa pregunta) y si logra contestar eso, es porque definitivamente lo ha hecho.

“Somos como un troll de las preguntas.”

Exacto, Manolo. Cuando menos se den cuenta, ya nos habrán contado todo lo que queríamos.

Puntos clave

Estos son **tips** de grandes rasgos a tener en cuenta para no morir en el intento.

Demasiadas preguntas pueden romper con la interacción debido a que va a sentir un acoso, el objetivo. Va a darse cuenta que necesitamos algo de él o que queremos controlarlo. Si la charla es tan inocente como queremos que crea, esto no sucedería. No sólo hay que hacer preguntas, sino también abrirse un poco al otro (recuerden el pilar de la confianza).

Muy pocas preguntas van a hacer que la otra persona se sienta incomoda. Imaginen si sólo hablamos, y hablamos, y hablamos. Ya sea de nuestra persona (quedando como un ególatra) o de la suya (pareceremos simples idiotas). Es bueno hablar lo justo y necesario, para hacer pequeños movimientos de confianza, pequeños gestos y pequeñas frases. Pero no queremos llamar la atención y que se desconcentre de si mismo.

Solamente hacemos **una pregunta a la vez,** demasiadas van a lograr que nuble la respuesta individual. Si hacemos varias preguntas puede pasar que sólo conteste una de ellas, o que se olvide alguna, o que nosotros no hayamos prestado tanta atención. Para no perdernos, poder llevar pregunta por pregunta sabiendo a donde ir y profundizando en cada pregunta que hacemos vamos a parecer unos verdaderamente interesados y no unos atacantes. Este tip beneficia ambas partes.

La mejor linea de preguntas seria:

1. **Neutrales**: “¿Conocés las 10 contraseñas más usadas?” podría ser una que saque una pequeña conversación sobre cuál es la que usa nuestro objetivo. Quizás, con algo de buenos timings, podamos llegar a realizar el ataque.
2. **Abiertas**: Suponiendo que no lo hemos logrado aún, pasamos a preguntar: “¿Qué tan fuertes pensás que son tus contraseñas?”. Aún nos vamos dirigiendo a eso, a poder llegar a tu objetivo.
3. **Cerradas**: En este escenario, el atacante todavía es un novato y como no logró estructurar confianza, el objetivo aún no nos dice cuál es el password. Por lo tanto podría preguntar “¿Alguna de tus contraseñas está dentro de la lista?”. Claro que es muy arriesgado, pero supongamos que la conversación se va llevando y el objetivo tiene confianza en ti pero el miedo suficiente como para no decir nada.
4. **Directas**: Saltamos a nuestro último recurso. Las preguntas directas. Estas son peligrosísimas. No se puede volver atrás si hicimos algo mal en esta fase, quizás hasta es mejor volver a empezar en la etapa 1 e intentar otro camino. Pero el ejemplo aquí sería: “¿Y qué contraseña usas para tu email?”. Está claro por qué es un límite a cruzar muy raro y no está del todo bien. Un buen elicitator, no debe llegar casi nunca a esta etapa. Aunque ya veremos otras maneras de conseguir lo que queremos.

Y un **último tip**. Preguntar “por que” puede hacer levantar las **defensas** de las personas, **automáticamente**. Esto suele ser malo a menos que estés investigando las técnicas de defensa que tiene esa persona para esquivar las preguntas. En ese caso es una buena herramienta. :D

REPASO GENERAL:

1. Necesitamos entender cómo nos debemos comunicar con la gente.
2. Debemos adaptarnos fácilmente, y llevar nuestra conversación a la adecuada, sabiendo tiempo y lugar.
3. Es de crucial importancia crear un lazo de confianza e intimidad con el objetivo.
4. La comunicación esta a la par del pretexto. Lo veremos en la próxima clase.
5. Debemos ser inteligentes para hacer las preguntas necesarias para lograr sacarles la información. Recuerden que las preguntas que se responden por “sí” o “no”, no suelen ser las correctas.

EEEEEEEjercicio para el hogar:

Vamos a conocer a una nueva persona y van a lograr que a través de preguntas, les cuente sobre algo muy íntimo. Algo que no quiera contar a nadie, o que les de acceso a un área restringida. Pueden contarles su experiencia en los comentarios :).

Pueden seguirme en Twitter: @RoaddHDC

Contactarse por cualquier duda a: r0add@hotmail.com

Para donaciones, pueden hacerlo en bitcoin en la dirección siguiente:

1HqpPJbbWJ9H2hAZTmpXnVuoLKkP7RFSvw

También recomiendo que se unan al foro: underc0de.org/foro

Roadd.