Phishing

El post anterior trataba sobre algunos factores de riesgo en las aplicaciones móviles y algunos controles básicos con los que abordarlos. Además de las amenazas que se nombraban en aquel post, existe otra más de la cual considero que es fundamental tener ciernas nociones, y es ésta la que me gustaría tratar en este último post. Es por ello que he seguido leyendo sobre la **Gestión del Riesgo Institucional en el Mundo Móvil**, y esta vez he investigado acerca del impacto que produce el **Phishing** en el **Mundo Móvil**.

¿Qué es Phishing?:

El termino **Phishing** es utilizado para referirse a uno de los métodos utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. Estos ataques se producen de la siguiente manera:

1. Todo comienza con un correo electrónico no deseado, o **spam**. Normalmente nadie acostumbraría a leer el correo electrónico no deseado, pero, puesto que a veces el correo legítimo no atraviesa los filtros y se queda con el no deseado, comprobar esta "bandeja" no resultaría extraño. Otra opción podría ser que el filtro de correo electrónico no hubiera sido capaz de detener el intento de estafa. Sea como sea, el destinatario del correo acaba leyendo el correo.
2. Este correo contiene una URL que direcciona al dominio del atacante, y se espera que el usuario que recibe el correo acceda a ella con una de las siguientes escusas:
    1. Cambio en la normativa del banco.
    2. Cierre incorrecto de la sesión del usuario.
    3. Mejoras en las medidas de seguridad.
    4. Detectada intrusión en sus sistemas de seguridad.
    5. Bloqueo de la cuenta por motivos de seguridad.
    6. Etc.
3. Una vez en el dominio del atacante, se espera que la víctima introduzca los datos que el atacante desea, para ello el atacante hace que su dominio se parezca, tanto en nombre como apariencia, al dominio al que la víctima cree estar accediendo.

Y además, según **un artículo de ElevenPaths** (la unidad global de ciberseguridad de Telefónica), es mucho más fácil atacar haciendo **Phishing** a una empresa a través de los **dispositivos móviles**. Las oportunidades que ofrecen los dispositivos a los atacantes para realizar ataques son las siguientes:

- **Las dimensiones de la pantalla:** Cuando el usuario entra a un sitio web el **dispositivo móvil** intenta ofrecer la mayor visibilidad posible en la pantalla. Esto hace que en algunos navegadores la barra de direcciones desaparezca rápidamente. No saber en qué página se está, aumenta el peligro y facilita la labor de los atacantes.

- **Las vistas incrustadas en las aplicaciones móviles:** Algunas aplicaciones de redes sociales como Facebook, Twitter, o los gestores de correo, utilizan vistas web embebidas con el fin de proporcionar comodidad al usuario y estética. Cargan la dirección URL enlazada desde la **aplicación móvil**, y por defecto no muestran la dirección URL en ningún lugar de la **aplicación móvil**.
- **Los subdominios:** Otro problema de espacio que presentan las barras de direcciones en los navegadores de los **dispositivos móviles** es que suele desplazar la vista de forma que se muestran normalmente los subdominios más a la izquierda. Este detalle permite al atacante diseñar en su sitio web un subdominio con, por ejemplo, un formato como el siguiente www.defensa.gob.es.dominiomalicioso.com. En este caso, si se accede desde Android al sitio web se vería lo siguiente:

- **Y qué ocurre con el SSL:** Se supone que el SSL, al igual que en cualquier ordenador, debería ser la mejor defensa contra el **Phishing**. ¿Lo ponen fácil en las versiones más

ligeras del navegador? En general, si la conexión no está cifrada, la barra de direcciones ni siquiera muestra el protocolo por el que se navega.

¿Qué podemos hacer?:

Los empleados de la organización deben estar concienciados de lo que un atacante es capaz de hacer mediante el **Phishing**. Por eso todo empleado tiene que saber que debe:

- **No lanzar la precaución por la ventana** cuando se cambia del ordenador al **dispositivo móvil**.
- **Evitar hacer clic en enlaces de mensajes SMS.**
- **Comprobar si una página está utilizando HTTPS**.

El **dispositivo móvil** no es más seguro, simplemente porque no es lo mismo que un ordenador. E independientemente desde qué dispositivo se facilita la información personal o una contraseña, si se hace en el sitio equivocado, esa información va a acabar en las manos de personas equivocadas…

Referencias:

Otros:

«¿QUÉ ES EL PHISHING?», Info Spyware, acceso el 27 de noviembre de 2016, https://www.infospyware.com/articulos/que-es-el-phishing/.

«Phishing en dispositivos móviles: ¿es más fácil?», ElevenPaths, acceso el 27 de noviembre de 2016, http://blog.elevenpaths.com/2013/11/phishing-en-dispositivos-moviles-es-mas.html.

«Phishing a través de SMS», naked security, acceso el 27 de noviembre de 2016, https://nakedsecurity.sophos.com/es/2016/02/12/phishing-via-sms-crooks-target-australian-mobile-banking-users/.