Seguridad en dispositivos móviles (Teléfonos, tabletas, etc.)

Ante la proliferación de uso de dispositivos móviles personales conectados a la red corporativa de la Universidad de Zaragoza, se recomienda unos requisitos de seguridad que hagan su uso compatible con las políticas de seguridad de la UZ. En la actualidad, estos aparatos se han convertido en herramientas imprescindibles para el trabajo, gracias a su movilidad y su conexión a Internet, lo que conlleva también nuevos riesgos para la universidad que los propios usuarios deben tener en cuenta.

Recomendaciones

- Poner contraseña a nuestros dispositivos, estableciendo bloqueo automático de pantalla, puede ser un PIN, patrón de desbloqueo, biométrica. (Ajustes, Seguridad, Bloqueo de pantalla), esto minimiza el problema con el **robo o pérdida** de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives.
- Utilizar redes Wi-Fi inseguras puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe. También podemos conectarnos a redes Wi-Fi que suplantan a redes Wi-Fi lícitas.
- Mantener nuestros dispositivos y las aplicaciones instaladas actualizadas, desinstalando las que no se utilicen (Play Store → Ajustes → Actualizar aplicaciones automáticamente en Android o en dispositivos IOS Ajustes → iTunes Store y App Store –> Descargas Automáticas →Activar aplicaciones), evitará la **infección por malware** pues el software malicioso puede robar información confidencial y credenciales de acceso a diferentes recursos.
- Los sitios web fraudulentos, la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen.
- No permitir la instalación de aplicaciones de origen desconocido. (Ajustes → Seguridad → Aplicaciones de origen desconocido).
- Si las tareas a realizar en el trabajo se trasladan al hogar deberán seguir manteniendo un aceptable nivel de ciberseguridad se recomiendan las siguientes medidas:
  - No se permitirán usos domésticos (juegos, descargas, etc.) por otros usuarios en el dispositivo utilizado como puesto de trabajo o estudio;
  - Se realizarán copias de seguridad de forma periódica.
  - En caso de utilizar una red Wi-Fi doméstica se seguirán las siguientes recomendaciones para protegerla y evitar accesos no autorizados:
    - ✓ utilizar cifrado WPA2 o WPA3 en caso de estar disponible y que los dispositivos sean compatibles;
    - ✓ utilizar una clave robusta (larga, con diversidad de caracteres, difícilmente adivinable).
    - ✓ desactivar la función WPS en caso de estar activa.
- Limitar los permisos en las aplicaciones (acceso a los contactos, imágenes, ubicación, micrófono.) procurando especialmente no habilitar la administración del dispositivo.
- Proteger nuestra cuenta con segundo factor de autentificación cuando sea posible. (Ajustes→ Google→Seguridad→Verificación en dos pasos en Android en IOS Ajustes→[Tu nombre]→Contraseña y seguridad→Autenticación de doble factor)
- No realizar modificaciones en el software del dispositivo. Los dispositivos Android e iOS cuentan con restricciones de fábrica que aumentan su seguridad y la de la información que manejan. Nunca hay que hacer Jailbreak o rootear un smartphone.
- Bloquear el dispositivo de manera remota en caso de perdida. La mayoría de sistemas operativos tanto para ordenador, como para móvil cuenta con funciones que lo permiten, generalmente a través de un panel de administración web.