

¿CÓMO EVITAR ATAQUES A TU MÓVIL CORPORATIVO?

APPS (Aplicaciones)

- Descarga solo aplicaciones que estén autorizadas por Brink's.
- Mantén actualizadas tus aplicaciones para evitar problemas de seguridad.
- Si ya no están disponibles en la tienda oficial, es mejor desinstalarlas.
- No concedas administración o permisos excesivos a las aplicaciones, salvo si confías en ellas.

Bluetooth

- Desactiva el emparejamiento automático del bluetooth.
- Desactívalo cuando no este en uso.

Navegador

- Mantente alerta frente a publicidad y concursos que aparentan ser demasiado buenos para ser reales. Frecuentemente re-direccionan a sitios maliciosos que parecen ser seguros.
- Pon atención frente a las direcciones URL's. Estas son difíciles de verificar en pantallas móviles.
- Nunca guardes tus claves cuando ingreses a un sitio web.

WIFI

- No conectes dispositivo a redes desconocidas.
- Siempre desactiva el wifi cuando no esté en uso.
- No envíes información sensible vía wifi a menos que estés seguro de estar conectado a una red confiable.

Smishing (Mensajes maliciosos vía SMS)

- No confíes en mensajes que te inviten a revelar sus contraseñas e información personal.
- Mucho cuidado con prácticas similares en plataformas como WhatsApp, Facebook, Messenger, Instagram, etc.
- Trate los mensajes de la misma manera que trataría el correo electrónico, ¡Siempre piense antes de hacer clic!

Vishing (Estafas telefónicas)

- No revele información financiera personal ni números de tarjetas de crédito por teléfono o email.
- Nunca haga clic en un enlace de correo electrónico comercial no solicitado.
- Al iniciar una llamada preocúpate que la comunicación es con otra persona y no con una grabación maliciosa.



Replica estas buenas prácticas en todos los dispositivos



No olvides utilizar métodos de contraseña segura como desbloqueo por huella y/o facial, para acceder a tu móvil y evitar robo de información.



Jorge Briones
Director de Tecnología, Nuevos
Negocios y Proyectos Estratégicos

