ACTIVIDAD PREVENCION DE CIBERATAQUES

Lee los siguientes casos de ciberataque, identifica que tipo de ciberataque es:

1. Durante un evento de ventas en línea, un sitio web de compras popular experimenta un ataque que resulta en la caída del sitio web y la imposibilidad de completar transacciones.

2. Los estudiantes y el personal de una institución educativa reciben correos electrónicos fraudulentos que parecen ser enviados por el departamento de TIC. Los correos electrónicos solicitan a los destinatarios que proporcionen sus credenciales de inicio de sesión en un sitio web falso que imita la página de inicio de sesión del sistema de gestión del aprendizaje.

3. Una universidad experimenta una infección en su red informática, lo que resulta en la pérdida de datos confidenciales de estudiantes y profesores.

4. Una empresa experimenta un ataque donde sus sistemas informáticos son infectados y todos los archivos se cifran. Los atacantes exigen un rescate en Bitcoin para desbloquear los archivos y restaurar el acceso.

5. Un estudiante instala una aplicación de juegos gratuita en su teléfono inteligente, que muestra anuncios emergentes en la pantalla de inicio y durante el juego.

6. Un usuario descarga una aplicación de seguimiento de ubicación para su teléfono inteligente, sin saber que rastrea su ubicación en tiempo real y envía la información a un servidor.

7. Un usuario hace clic en un anuncio en línea que promete acceso gratuito a un programa de televisión popular, sin saber que el enlace lleva a una página web infectada que cifra todos los archivos en su computadora y exige un rescate para recuperarlos.

8. Un estudiante instala un programa de chat en su computadora portátil, sin saber que graba todas sus conversaciones sin su conocimiento.

9. Un usuario recibe una llamada telefónica de alguien que se hace pasar por un representante de soporte técnico de su proveedor de servicios de Internet. El llamador solicita acceso remoto al dispositivo del usuario para "solucionar problemas".

10. Un empleado de una empresa recibe un mensaje de texto que parece ser de su banco, solicitando que haga clic en un enlace para verificar su cuenta. Al hacerlo, su dispositivo se infecta con un programa que roba sus credenciales bancarias.