Consejos para un teletrabajo seguro

La protección contra el COVID19 también tiene que ser online.

TIPS PARA DETECTAR UN PHISHING:

- Sospecha si el contenido del mensaje tiene **fallos de escritura** o errores gráficos.
- Un mensaje fraudulento **no suele estar personalizado**. Utilizan saludos genéricos para poder estafar a un número elevado de personas.
- **Evita abrir enlaces o archivos adjuntos** sobre el coronavirus. Y desconfía de aquellos descargables con más de una extensión (".zip" o ".exe").
- **Fíjate en el asunto del mensaje**. Sospecha si está relacionado con el coronavirus y es llamativo: "atención coronavirus", "alerta coronavirus" o "medidas de seguridad ante el coronavirus", por ejemplo.
- Asegúrate que el **enlace en el que vas a clicar sea el oficial de la página que quieres visitar**.
- Para informarte adecuadamente **confía solo en fuentes oficiales y en medios de comunicación contrastados**. Esta información oficial no debería provenir de correos electrónicos.

TELETRABAJAR DE FORMA SEGURA: ¿CÓMO NOS PROTEGEMOS?

- Utiliza **equipos corporativos**
- Utiliza **VPN** (Red Privada Virtual) para conectarte de forma remota a los sistemas de tu organización.
- Utilizar tecnologías de **doble factor de autenticación**.
- Contar con **contraseñas robustas**, individuales y conocidas solo por ti.
- Disponer de **antivirus** instalado en equipos de trabajo.
- Trabajar con **redes wifi privadas**.
- Realizar **copias de seguridad** de forma periódica.
- Llevar a cabo **actualizaciones periódicas** de los sistemas y aplicaciones.