UD07 - Correu electrònic i ferramentes de comunicació Microsoft 365

UD07 Pr3 .- Crear documento compartido Word

Primero debéis crear grupos. A continuación tenéis que crear un documento

compartido entre los miembros del grupo (2-3 alumnos por grupo), y trabajar

sobre el archivo a la vez. Después debéis realizar las siguientes tareas:

1. Indicar los diferentes tipos de fraudes que existen (phishing…), dando una explicación de los mismos y el modus operandis.
   - **Estafa nigeriana:** Este timo se basa en el uso indebido del email marketing, donde la víctima recibe correos electrónicos donde le ofrecen grandes sumas de dinero.
   - **Fraude Romántico:** El modus operandi se basa en enamorar a una persona por medio del Internet, mayormente mediante el mal uso de las redes sociales, creando perfiles falsos con imágenes y videos dedicados a engañar, por lo tanto, la víctima nunca llega a conocer al estafador.
   - **Fraudes en compras online:** La operatividad de este tipo de fraudes, es precisamente, ofrecer productos vía online a precios mucho más bajos respecto a las referencias de los mercados, desde una tienda digital.
   - **Phishing:** Su operatividad se basa en el envío de mensajes de texto y/o WhatsApp y, por correo electrónico, copiando links falsos de páginas web que son similares a los sitios que el usuario frecuenta, es decir, crean una réplica del sitio web para que coloquen sus datos personales y así obtenerlos.

2. Hacer un resumen de los consejos de seguridad.
   - Asegúrate de quién te está enviando los correos electrónicos, y en caso de alguna duda, comunícate directamente con el servicio de atención al cliente de esa empresa con los teléfonos de contacto oficiales.
   - Verifica si se trata de un sitio web reconocido y legal de citas. Pídele a la persona que active su función de "ubicación" y que mande una imagen de la ubicación actual en movimiento desde el WhatsApp.
   - Antes de hacer compras vía web, investiga previamente el dominio para evitar riesgos. Solo haz compras en páginas web conocidas y a vendedores con buena reputación, ¡nunca a alguien con gestiones negativas! Verificar los comentarios de otras compras. Haz muchas preguntas acerca del producto y el vendedor.
   - Descargar un antimalware para defenderte. No abrir archivos adjuntos en emails no solicitados. No proporcionar información personal ni contraseñas por ningún medio. Mantener actualizado el navegador y aplicar los parches de seguridad.

3. Indicar qué es la identidad digital, y contestar a las preguntas ¿cómo afecta? Y ¿cómo protegerla?
   La identidad digital es la versión en Internet de nuestra identidad física y está compuesta por una gran cantidad de datos que proporcionamos en la red: datos bancarios, fotografías, preferencias a la hora de comprar online, correo electrónico, etc.
   La identidad digital, se construye desde un sin número de fuentes y se determina la mayoría de las veces por juicios anónimos de valor. Así pues, lo que antes podía quedar en un entorno social reducido (la familia, trabajo, amigos) ahora se distribuye de forma masiva y puede afectar de manera irremediable el concepto social que proyecta una particular, un personaje público, una empresa o institución cualquiera.
   ¿Cómo proteger nuestra identidad digital?
   - No utilices redes wi-fi desprotegidas o públicas. ...
   - No utilices páginas web desprotegidas. ...
   - Utiliza contraseñas seguras y cámbialas regularmente. ...
   - Actualiza tu software regularmente. ...
   - Repasa los permisos y las políticas de privacidad. ...
   - Monitoriza tu nombre regularmente.

4. ¿Qué es el CVV de una tarjeta de crédito?
   El código CVV o CVC es un grupo de 3 o 4 números situado en el reverso de la tarjeta de crédito o débito. Dicho código se utiliza como método de seguridad en transacciones en las que la tarjeta no está físicamente presente, como en compras por teléfono o internet. Es esencial realizar un uso responsable y seguro de la tarjeta, así como tener bajo control los gastos para cuidar la salud financiera.

5. ¿Por qué utilizar un gestor de contraseñas? ¿cuál utilizaríais?
   Un gestor de contraseñas es la opción más segura para almacenar las credenciales. Todas las claves se guardan cifradas y solo se puede acceder a ellas conociendo la contraseña maestra. Estos gestores de contraseñas permiten clasificar las mismas según su categoría, donde se irían creando las diferentes entradas con los usuarios y contraseñas de cada servicio que utilizamos. Con esto, dispondremos de una herramienta segura que nos permitirá tener contraseñas robustas sin tener que acordarse de todas ellas, repetirlas o apuntarlas.
   Teniendo todo esto en cuenta será mucho más fácil mantener las credenciales a salvo de terceros malintencionados.
   Utilizaría **DASHLANE**.
6. Compartir el documento con el profesor, en modo solo lectura, sin privilegios de escritura.

NOTA: Recordar utilizar la guía de estilos, y poner los nombres de los diferentes componentes del documento en el mismo.