Solucionario / CTRD0004

Herramientas básicas de productividad y colaboración en dispositivos móviles

Soluciones

Actividades

Test de Repaso

CEP

SOLUCIÓN ACTIVIDADES

MÓDULO 1. HERRAMIENTAS BÁSICAS DE COMUNICACIÓN EN DISPOSITIVOS MÓVILES

SOLUCIÓN ACTIVIDAD 1

«Face ID» es una tecnología de reconocimiento facial desarrollada por Apple para sus dispositivos, como el iPhone. Esta tecnología utiliza un sistema especial llamado cámara TrueDepth, que puede proyectar más de 30,000 puntos invisibles sobre tu cara para crear un mapa detallado de tu cara. Este mapa es único para cada persona, al igual que nuestras huellas dactilares son únicas.

Además de crear un mapa de tu cara, la cámara TrueDepth también captura una imagen infrarroja de tu cara. La luz infrarroja es una luz que no podemos ver, pero que la cámara puede detectar. Esta imagen infrarroja proporciona información adicional sobre la forma y las características de tu cara.

Cuando «Face ID» captura los datos de tu cara, estos datos se convierten en una especie de fórmula matemática. Este proceso se realiza utilizando una parte especial del chip de tu teléfono, que es como el cerebro del dispositivo. Esta parte especial se llama «motor neuronal» y está diseñada para realizar cálculos complejos muy rápidamente. Esta fórmula matemática se guarda en una parte segura del chip de tu teléfono, llamada «Secure Enclave». Puedes pensar en el «Secure Enclave» como una caja fuerte en tu teléfono donde se guardan los datos más sensibles, como la fórmula matemática de tu cara.

La representación matemática de tu cara se compara con los datos faciales que has registrado en tu dispositivo. Si los dos coinciden, el teléfono sabe que eres tú y se desbloquea. Este proceso ocurre en una fracción de segundo, por lo que parece que tu teléfono se desbloquea instantáneamente cuando lo miras.

«Face ID» puede adaptarse a los cambios en tu apariencia. Por ejemplo, si un usuario decide dejarse barba, «Face ID» notará el cambio y actualizará el mapa de su cara. Si hay un cambio más significativo en la apariencia, como, por ejemplo, afeitarse una barba completa, «Face ID» pedirá confirmar la identidad usando el código de acceso antes de actualizar los datos faciales.

«Face ID» también puede funcionar en diferentes condiciones. Puede funcionar con sombreros, bufandas, gafas, lentes de contacto y muchas gafas de sol. Además, puede funcionar en interiores, exteriores e incluso en total oscuridad. Con la actualización de iOS 15.4 y en los modelos de iPhone 12 o posteriores, «Face ID» incluso puede reconocerte si llevas una mascarilla.

Para empezar a usar «Face ID», primero tienes que enseñarle a tu teléfono cómo es tu cara. Esto se hace en la configuración de tu teléfono, donde encontrarás una opción para registrar tu cara. Una vez que tu cara está registrada, puedes desbloquear tu teléfono simplemente mirándolo.

SOLUCIÓN ACTIVIDAD 2

Dado que no hay solo una respuesta correcta, una respuesta válida podría ser la siguiente:

- Google Meet: es una solución de videoconferencia segura y fácil de usar que se integra perfectamente con otras herramientas de Google Workspace. Permite realizar reuniones instantáneas, compartir pantalla y documentos, y revisar informes y análisis basados en los resultados de las conferencias. Además, Google Meet es gratuito para usar a través de tu cuenta de Google, aunque también ofrece características premium

para empresas que necesitan un soporte de colaboración adicional. Link: (https://workspace.google.com/products/meet)

- TeamViewer Meeting: es una herramienta de videoconferencia basada en la nube para reuniones en línea y videoconferencias. Con aplicaciones para Windows, macOS, Android e iOS, y la capacidad de unirse a una reunión a través de un navegador web sin necesidad de instalar un complemento, TeamViewer Meeting se esfuerza por ser el mejor software de videoconferencia para empresas que trabajan de forma remota. Link: www.teamviewer.com/es/legal/product-descriptions/teamviewer-meeting.

- Zoho Meeting: una solución de videoconferencia en la nube que permite a las empresas y a sus colaboradores realizar reuniones de video o audio, mantener sesiones con hasta 1,000 asistentes, compartir pantallas, usar una pizarra, grabar reuniones y realizar encuestas en vivo a los asistentes. Link: www.zoho.com/es-xl/meeting.

- CyberLink U Meeting: es una aplicación de videoconferencia diseñada para la comunicación empresarial dinámica. Ofrece una gran cantidad de características, incluyendo compartir pantalla, grabación de sesiones, múltiples anfitriones, gestión de usuarios, videos fijados, función de "levantar la mano" en las reuniones, chat de reuniones con notas, pizarras colaborativas, fondos virtuales, transcripciones de reuniones, informes y análisis. Link: https://u.cyberlink.com/products/umeeting.

- Webex Meetings: es la plataforma de videoconferencia de Cisco, diseñada para permitir a los equipos de negocios colaborar de manera eficiente. Ofrece video y audio de alta definición y características de software, incluyendo compartir pantalla, pizarras, reuniones ilimitadas uno a uno o en grupo, y salas de reuniones. Webex Meetings es altamente escalable y está diseñado para funcionar para profesionales individuales y agencias gubernamentales por igual. Link: www.webex.com/es/video-conferencing.html.

SOLUCIÓN ACTIVIDAD 3

Una respuesta válida podría ser la siguiente:

- Phishing: esta técnica de ciberdelincuencia implica el envío de correos electrónicos que parecen provenir de entidades legítimas con el objetivo de engañar a las personas para que proporcionen información confidencial. Es común en el phishing el uso de páginas web falsas que imitan a las de las entidades legítimas.
- Smishing: es una variante del phishing que utiliza mensajes SMS en lugar de correos electrónicos. En el smishing, se envían mensajes de texto con enlaces a sitios web fraudulentos o números de teléfono con el objetivo de engañar a las personas para que revelen información personal o financiera.
- Vishing: esta técnica proviene de la combinación de voice y phishing y se refiere a los ataques de phishing que se realizan a través de llamadas telefónicas. En el vishing, las personas que realizan el ataque se hacen pasar por representantes de una entidad legítima y solicitan información confidencial durante la llamada.

La mejor defensa contra estos ataques es siempre ser cauteloso y no proporcionar información personal a menos que se esté seguro de la identidad de la otra parte. Es importante recordar que ninguna entidad legítima solicitará información confidencial por estos medios.

SOLUCIÓN ACTIVIDAD 4

Aunque a veces se usan indistintamente, en rigor, emojis y emoticonos son cosas distintas: los emoticonos son construcciones creadas mediante caracteres del teclado, mientras que los emojis son pequeñas imágenes que representan distintos elementos y emociones. Además, aunque los emojis tienen sus raíces en los emoticonos, se

han desarrollado de manera independiente y ahora representan una amplia gama de emociones, objetos e ideas.

Los emoticonos surgieron en la década de 1980 con la aparición de los mensajes de texto y la comunicación en línea. Son combinaciones de signos o letras del teclado que representan una expresión facial que simboliza un estado de ánimo. Por ejemplo, el emoticono «:-)» representa una cara sonriente.

Por otro lado, los emojis son pequeñas imágenes o iconos digitales que se utilizan en la comunicación digital para expresar emociones, ideas, objetos, entre otros. Son una invención más reciente que los emoticonos. El término «emoji» es de origen japonés, formado por «e», que significa dibujo, y «moji», que significa carácter escrito. Los emojis fueron creados en 1999 por el diseñador Shigetaka Kurita, quien trabajaba para una compañía telefónica japonesa que buscaba una forma de comunicación más visual y rápida para sus clientes. Así, nacieron los primeros emojis, que incluían imágenes de comida, clima y emociones.

MÓDULO 2. USO DE LAS REDES SOCIALES EN DISPOSITIVOS MÓVILES

SOLUCIÓN ACTIVIDAD 1

Una respuesta válida sería la siguiente:

Ante esta situación, mi primera reacción sería de escepticismo. El perfil parece sospechoso (foto de perfil genérica, pocos seguidores, sigue a muchas personas, y no hay contenido original), y me hace cuestionar su autenticidad. Para confirmar mis sospechas, buscaría si el perfil tiene una insignia de verificación. En Facebook, los perfiles verificados tienen un pequeño tick azul junto al nombre de la persona, lo que indica que el perfil ha sido confirmado como auténtico por la plataforma.

Si después de revisar el perfil sigo pensando que es falso, informaría de él a Facebook. Facebook tiene políticas y procedimientos para manejar los perfiles falsos y suele tomar medidas para eliminarlos. Finalmente, evitaría interactuar con el perfil falso. No respondería a los mensajes no solicitados ni aceptaría la solicitud de amistad.

Por otro lado, aun en el caso de que la persona pareciera legítima, nunca compartiría información sensible (personal, financiera, etc.) con ella, al ser desconocida. Si tengo dudas, siempre es mejor errar por el lado de la precaución.

SOLUCIÓN ACTIVIDAD 2

El término hashtag en el contexto de las redes sociales fue propuesto por primera vez por Chris Messina, un diseñador de productos de Silicon Valley. En 2007, Messina sugirió en Twitter (hoy X) el uso del símbolo # para agrupar temas o conversaciones. Su primer tuit con

un hashtag fue: «How do you feel about using # for groups. As in #barcamp [msg]?». Desde entonces, el uso del hashtag se ha extendido a todas las redes sociales y se ha convertido en una herramienta esencial para agrupar contenido relacionado y facilitar la búsqueda de temas específicos.

El símbolo #, también conocido como «numeral» o «almohadilla», tiene una larga historia antes de su uso en las redes sociales. Se utilizó en los teclados de los teléfonos en los años 60 y en el lenguaje de programación C en 1978. En el lenguaje de programación, el símbolo # se usaba para palabras clave especiales que debían ser procesadas antes que nada por el preprocesador de C. De ahí proviene el nombre hash, que se unió con tag (etiqueta en inglés) para formar el término hashtag.

SOLUCIÓN ACTIVIDAD 3

El concepto de «Me gusta» o «Like» en las redes sociales tiene sus raíces en la plataforma FriendsFeed, que se lanzó en 2007. Leah Pearlman, una diseñadora que trabajaba en FriendsFeed, tuvo la idea de crear un botón que permitiera a los usuarios marcar ciertas publicaciones que les gustaban. En sus primeras iteraciones, FriendsFeed utilizó el símbolo del corazón para representar esta funcionalidad.

El equipo de Facebook vio el potencial de esta función y decidió incorporarla en su propia plataforma. Sin embargo, el camino hacia el botón «Me gusta» que conocemos hoy no fue directo. El proyecto se asignó a Jonathan Pines, Jared Morgernstern y Soleio Cuervo, quienes tuvieron que convencer a Mark Zuckerberg de que la función no disminuiría la interacción en la plataforma, sino que la aumentaría.

Inicialmente, la función se llamaba «Awesome button» y se consideraron varios símbolos para representarla, incluyendo las estrellas, el símbolo de suma ('+') y un pulgar hacia arriba. Aunque el pulgar

hacia arriba fue finalmente seleccionado, hubo preocupaciones debido a que en algunas regiones del mundo este gesto no se considera positivo.

Finalmente, el 22 de agosto de 2007, se propuso cambiar el nombre de la función de «Awesome» a «Like». Desde entonces, el botón «Like» se ha convertido en un elemento esencial en las redes sociales, permitiendo a los usuarios expresar su aprecio por el contenido y proporcionando una forma sencilla de interactuar. El botón «Me gusta» ha cambiado la forma en que nos comunicamos en línea, permitiéndonos compartir nuestras reacciones y sentimientos de una manera rápida y fácil. Hoy en día, es difícil imaginar las redes sociales sin la opción de «Me gusta».

SOLUCIÓN ACTIVIDAD 4

Una posible respuesta válida sería la siguiente:

El hashtag stuffing es una práctica en la que se incluyen demasiados hashtags en una publicación o mensaje en redes sociales con el objetivo de aumentar la visibilidad o el alcance. Aunque los hashtags pueden ser útiles para categorizar contenido y facilitar su búsqueda, el hashtag stuffing excesivo puede resultar molesto para los usuarios y afectar negativamente la experiencia en línea. Un ejemplo ficticio de hashtag stuffing en un tuit sería el siguiente:

> ¡Nuevo artículo en mi blog!
>
> #Moda #Tendencias #Estilo #OutfitDelDía #Fashionista #StreetStyle #Belleza #Maquillaje #Peinados #Zapatos #Accesorios #LookDelDía #Inspiración #FashionBlogger #FashionAddict #FashionGoals #FashionInspo #OOTD #InstaFashion #FashionLover #FashionLife #FashionPassion #FashionObsession #FashionistaLife #FashionForever
>
> ¡Lee más en el enlace de mi perfil!

En este ejemplo, la persona que ha escrito el tuit ha utilizado una gran cantidad de hashtags relacionados con la moda y el estilo. Aunque algunos hashtags son relevantes, la acumulación excesiva puede dificultar la lectura y dar la impresión de que se está intentando forzar la visibilidad del contenido. Es importante encontrar un equilibrio y usar hashtags de manera estratégica para que sean efectivos sin abrumar a los seguidores.

SOLUCIÓN TEST DE REPASO

1. a) La prevención del acceso autorizado a tu cuenta

2. b) Anuncios intersticiales

3. d) Todas las respuestas anteriores son correctas

4. d) Asíncrona

5. c) Correo electrónico

6. c) «Asunto»

7. c) Emoji

8. d) Reconocer que existe un problema

9. d) La dependencia excesiva de la tecnología

10. b) La posibilidad de divulgar involuntariamente información pública

11. d) Hashtag

12. d) Todas las respuestas anteriores son correctas

13. c) El símbolo # seguido de texto sin espacios

14. b) Menos de un minuto

15. d) Personalizar el contenido que se muestra a cada persona usuaria

16. d) Todas las respuestas anteriores son correctas

17. b) Pequeños archivos de texto que las redes sociales colocan en un dispositivo para rastrear el comportamiento en línea de una persona usuaria

18. c) Publican contenido muy original y singular

19. d) Xing

20. a) Ser informales