GIBBERFISH INICIO RÁPIDO

¡Bienvenido a Gibberfish! Nuestro enfoque es sobre su privacidad y seguridad pero necesitamos que seas un participante igual. A continuación se muestran un par de sugerencias para empezar.

PERFIL

Si es tu primera vez iniciar sesión debe tomar unos minutos para completar su perfil y mientras estás allí cambiar su contraseña Haga clic en el ⚙ en la parte superior derecha de la esquina y seleccionar **Personal** para editar tu perfil.

FRASES DE ACCESO

Buenas contraseñas son muy importantes para salvaguardar sus datos. Nosotros y muchos expertos en seguridad recomiendan crear contraseñas mediante el método Diceware. **Este es el único método** de generación de contraseña que se considera seguros. Su fácil de hacer y proporciona claves muy fuerte que pueden derrotar incluso a los adversarios más ingeniosos.

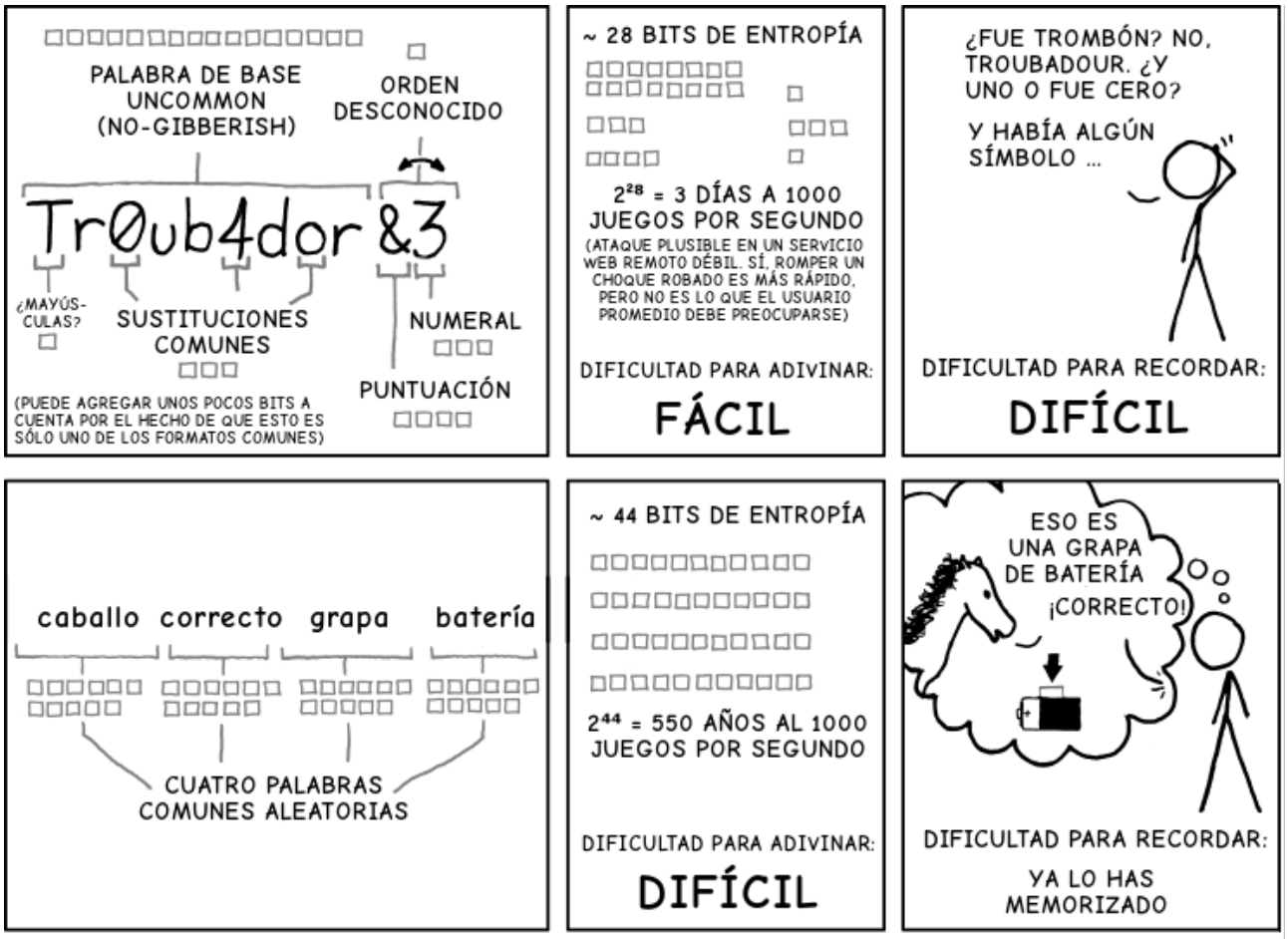


imagen cortesía de xkcd.com.

Mientras que el cómic anterior explica el concepto, el método Diceware recomienda una longitud de frase de paso de **5 o más palabras** para una seguridad óptima.

Nunca utilices una contraseña para el inicio de sesión de Gibberfish que utilices en otro lugar.

Siempre genera una contraseña única para cualquier servicio cuenta o dispositivo.

AUTENTICACIÓN DE DOS FACTORES

Una vez que has cambiado tu contraseña, también le animamos a habilitar la autenticación de dos factores ("2FA"). Se trata de instalar una aplicación en su dispositivo móvil que genera un código único de 6 dígitos en que debe ingresar cada vez que inicie sesión. Para que alguien pueda hackear su cuenta, necesitan conocer su contraseña y poseer físicamente el teléfono. Esta combinación te mantiene más seguro. Porque Gibberfish es parte del ecosistema de Nextcloud, puede utilizar la aplicación de Nextcloud 2FA. Esta aplicación es compatible con FreeOTP, que puede descargarse en la app store para dispositivos iOS y Android.

BÓVEDAS DE CLAVE

Si no está ya en el hábito de hacerlo sería una buena idea para guardar tus contraseñas en una bóveda clave como KeePass. Claves bóvedas hacen fácil de recordar con seguridad todas tus contraseñas. Se necesita bloquear su clave bóveda sí mismo con una frase de Diceware generado. Además recomendamos **fuertamente** que activar el cifrado de disco completo en el dispositivo de almacenamiento de su bóveda clave.

Este método asegura sólo necesita recordar una contraseña: uno para abrir su caja fuerte de claves.

HIGIENE DIGITAL

Buena higiene Digital es el uso consistente de prácticas de seguridad robusta.

Entendemos por robusto procedimientos que se han establecido o validada por expertos en seguridad de confianza. Éstos incluyen pero no se limitan a el proyecto de Electronic Frontier Foundation EFF el proyecto guardián y Tor.

Utilizamos consistente para enfatizar que el uso intermitente de cualquier práctica de seguridad es tan malo como no utilizando uno. Una vez que desarrolla un modelo de amenaza y una estrategia para derrotarlo debe aplicar esta estrategia **cada vez** que usted participar en las actividades privadas.

AMENAZAS

Comprender las amenazas que usted y su grupo encontrará es un paso importante en el establecimiento de una estrategia de seguridad útil. El objetivo es utilizar sólo las técnicas necesarias para proteger contra sus adversarios probablemente. Esto evitará que su régimen de seguridad ser tan onerosas que dejas de usarlo. El administrador puede ya han creado un modelo de amenaza que describe los retos de seguridad que usted y su grupo pueden esperar. Si no está seguro por favor contactar con ellos y preguntar.

Cada usuario debe entender el modelo de amenaza de su grupo y utilizar constantemente las mismas prácticas de seguridad.

Para obtener más información sobre modelos de amenaza, consulte este excelente primer producido por la EFF.

COMUNICACIONES EXISTENTES

Es probable que agregue Gibberfish a una variedad de cuentas existentes y servicios asociados con sus actividades en línea. Estas más viejas cuentas y servicios ya pueden verse comprometidas. Recomendamos utilizar cuentas frescas para cualquier actividad que implique su servidor Gibberfish el contenido almacenado allí o las actividades asociadas con él.

Reconocemos que esto no es siempre conveniente o apropiado para cada usuario. En este caso por favor tome el tiempo para volver a fijar cualquier cuenta o servicio que vaya a utilizar para actividades privadas. Cambiar sus contraseñas para cierre no autorizado de usuarios que pueden haber accedido sin su conocimiento. Siempre que sea posible permitir la autorización de dos

factores. Busque actualizaciones de software para todos sus dispositivos incluyendo su teléfono e instalarlos.

TOR

Usando Tor es la mejor manera para proteger su privacidad en línea. Por esta razón usan Tor para implementar el servidor de Gibberfish. Mientras que específicamente se refiere al proyecto de cebolla de la fresadora, Tor ha llegado a abarcar una gran variedad de productos y servicios personas pueden usar para proteger sus actividades en línea. Recomendamos que cada uno use el navegador Tor para anonimizar su presencia online.

Por favor lea cuidadosamente la documentación y FAQ que Tor proporciona sobre navegación en la red. Tienen importantes recomendaciones para mantener su privacidad. Importante usando el navegador Tor no garantiza que todas sus actividades en línea son anónimos.

Ya que su seguridad necesita escalar Tor tiene otras herramientas gratuitas para ayudar a. Cuando se evalúa el modelo de amenaza, puede investigar servidores puente y colas. Servidores de puente permiten a la gente a Tor en países que bloquearlo. Colas es un sistema operativo Linux, con programas utilizados, todo en una memoria USB. Permite el trabajo informático muy privado.

Descubra estos y otros servicios de Tor
https://www.torproject.org/projects/projects.html.en

LLAMADAS DE VÍDEO

La aplicación de Talk de Nextcloud le permite crear y unirse a llamadas de vídeo en su navegador. Para un mejor rendimiento en dispositivos móviles recomendamos que instale y utilice la aplicación móvil Nextcloud Talk que está disponible en iTunes, Google Play y FDroid.

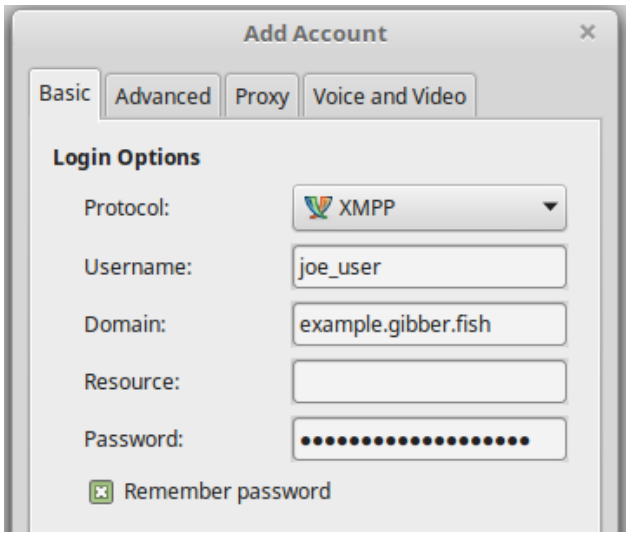
CHAT

El sistema de chat utiliza el protocolo estándar XMPP que te permitirá chatear con otros usuarios de Gibberfish pero también con cualquier otra persona en el mundo que utiliza un servidor XMPP. Su dirección XMPP es <su nombre de usuario>@<su servidor gibberfish>. Por ejemplo,

joe_user@example.gibber.fish

Cuando inicie una sesión en primer lugar tu lista de chat a la derecha de la pantalla aparecerá vacía. Desde el menú en la parte inferior se puede **Agregar contacto**. Simplemente comience a escribir y buscará automáticamente para los usuarios existentes en el servidor o puede escribir la dirección de XMPP de usuarios externos.

Para permanecer conectado cuando usted no está registrado en Gibberfish también puede conectarse al servidor directamente usando a un cliente compatible con XMPP como Adium, Pidgin o una de muchas de las aplicaciones móviles.



El servidor de chat también es accesible como un Tor "servicio de cebolla" en el puerto 5222. Consulte a su administrador por la dirección del servidor Tor.

Sin embargo al charlar con los usuarios fuera de su servidor usted tiene ninguna garantía de privacidad a menos que tú **y** tus contactos utilizan un plugin de endtoend cifrado como OTR. La mayoría clientes de chat compatibles con el cifrado endtoend y guías para ayudarle a entender y poder.

CLIENTES MÓVILES Y DE ESCRITORIO

Gibberfish trabaja con el Nextcloud le permite automáticamente sincronizar archivos desde el servidor y clientes móviles y de escritorio. Esto está deshabilitado por defecto como medida de seguridad. Si desea utilizar a estos clientes hable con su administrador de cambiar las reglas de acceso de archivo. Si decides sincronizar archivos localmente sólo hacerlo si activado el cifrado de disco completo para su dispositivo. Esto protege tus archivos si tu dispositivo es perdido robado o hackeado.

Es difícil pero posible que los datos a ser interceptada por adversarios ingeniosos mientras está en tránsito. Por esta razón **no recomendamos** sincronizar sus datos sin considerar cuidadosamente el modelo de amenaza y sus prácticas de seguridad.

MÁS LECTURA

Para documentación más extensa de las características de base consulte el Manual del usuario Nextcloud que también se encuentra en su carpeta de inicio de Gibberfish.

Los administradores también deben familiarizarse con el Manual de administración.

Por último le recomendamos suscribirse al Gibberfish Blog en la aplicación de noticias para mantenerse al día sobre importantes anuncios y nuestra declaración de Canarias.

NOTAS FINALES

Esperamos que disfrute usando Gibberfish. Hemos trabajado duro hacer lo fácil y segurouso de plataforma como los muchos contribuidores independientes para los distintos proyectos de código abierto que hemos integrado en nuestro servicio. Un agradecimiento especial para la gente de Nextcloud sin que nuestra plataforma no sería posible.

Contamos con donaciones para sobrevivir. Si usted puede permitirse lo por favor considere hacer una contribución caritativa de cualquier cantidad en https//gibberfish.org/es/donate. Lo agradeceremos inmensamente. Gracias

Por razones de seguridad nos sólo responder a las solicitudes de su administrador registrado. Si usted tiene preguntas relacionadas con el servicio por favor consulte a su administrador.