**Usando OTP en WordPress y Gmail**

[**junio 8, 2015**](https://hacking-etico.com/2015/06/08/usando-otp-en-wordpress-y-gmail/) / [**Manuel Camacho**](https://hacking-etico.com/author/kmx0/) / [**No comments**](https://hacking-etico.com/2015/06/08/usando-otp-en-wordpress-y-gmail/#respond)

Hoy retomo la publicación en el blog con un tema sobre contraseñas. Como sabéis, usamos contraseñas para todo, y es que los servicios Web como correo, redes sociales o banca online, así nos lo exigen. Por ello, el uso de contraseñas está muy masificado. Usamos contraseñas para todo. Menos seguras de lo que creemos pero se utiliza ese método que impide que cualquiera pueda entrar libremente a tus servicios de redes sociales, de banca, portales Web, equipos, etcétera…

No obstante, hay una falsa creencia de que usar contraseñas sean como sean, es estar seguros.

Evidentemente este pensamiento es erróneo y ocasiona muchos problemas de confidencialidad, suplantación de identidad, etcétera… Puestos en la piel del “pasota”, como me encuentro muy a menudo podríamos pensar “Es que nadie tiene que entrar en mi cuenta…” toma ya. Esto no es una ocurrencia mía para complementar el artículo sino que son palabras textuales que me han dicho en persona. Claro, y nadie tiene que robar coches, ni casas, ni negocios ni nada y sin embargo pasa. Pongamos la cosa difícil y al menos, cuando vean las dificultades, la tomen con otro ¿no?. Probemos pues  “Usando OTP en WordPress y Gmail”



Pues bien, el post no trata del uso de contraseñas fuertes, es decir, letras, símbolos, mayúsculas, minúsculas y números, que eso ya lo obviamos en nuestro blog, sino otros métodos que fortalezcan la autenticación.

El método al que vamos a hacer referencia es la autenticación OTP (One Time Password) o lo que es lo mismo, uso de una contraseña dinámica extra en nuestro login de, por ejemplo, WordPress. A la contraseña estática de siempre se le añade una contraseña temporal que dura, dependiendo la configuración, 1 minuto, 2, 3, 4…

Es decir, cuando vamos a acceder a nuestra panel de administración o zona privada, en la que nos pide la habitual password, si configuramos un método OTP, nos pedirá una contraseña temporal que se genera externamente y que está sincronizada con nuestra cuenta.

**¿Pero por qué OTP?**

OTP soluciona en parte, las deficiencias que se asocian con la contraseña de toda la vida. No son vulnerables a ataques de “replay” por tanto un atacante no puede reinyectar nada.

Otro punto fuerte es que usando contraseñas OTP, hacen al sistema mucho más robusto a ataques por fuerza bruta. No evita que se pueda desenmascarar la contraseña estática o incluso la OTP pero como es temporal, que dura 1 minuto según nuestras configuraciones hace que, si hubiera éxito en el descubrimiento de las credenciales, haya que empezar de nuevo porque la OTP cambia constantemente.

**¿Qué problema tiene?**

Básicamente que cómo hay que generar aleatoriamente infinidad de contraseñas OTP memorizarlas es misión imposible. Cuesta ya memorizar una credencial robusta con que memorizar una serie de decenas de claves…

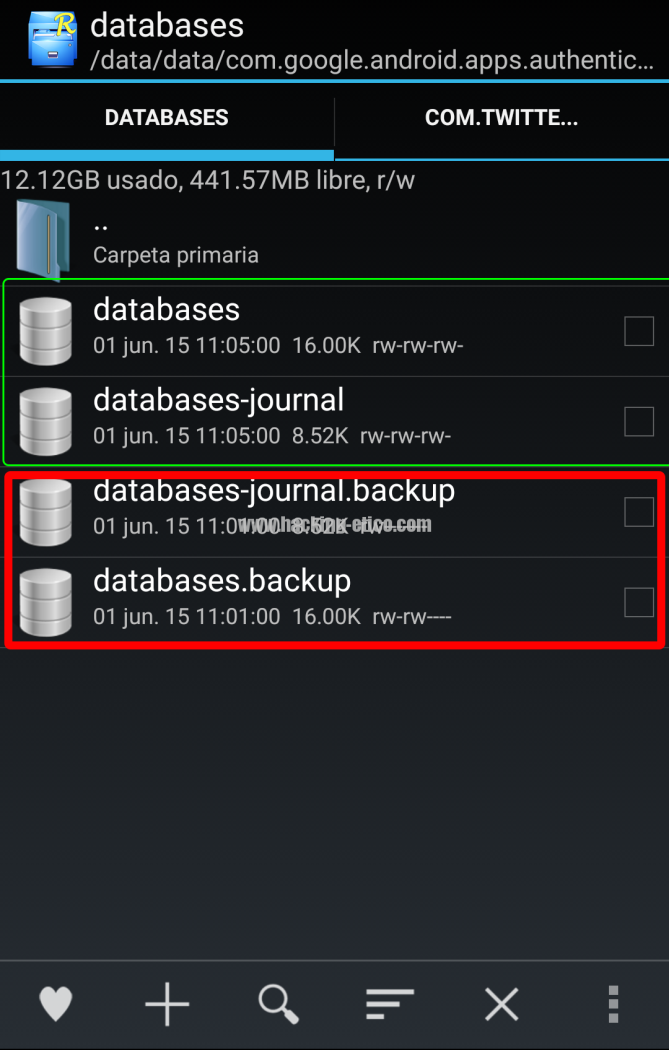
Para esto, se necesita un sistema externo, como Google Authenticator que se asocia perfectamente a por ejemplo, WordPress.

Podemos usar métodos sin APPs externas como la mencionada, ya que por ejemplo, si resetearamos el móvil perderíamos la “sincronización” APP-Servidor mediante la Key secreta.

Extra:

Aunque esto anterior podemos solucionarlo exportando la BBDD de Google Authenticator. Para ello necesitamos tener rooteado nuestro Android. Tenemos que hacer un backup del fichero “databases” ubicado en /data/data/com.google.android.apps.authenticator2

Cuando restaures tu teléfono, en el mismo directorio de tu terminal después de instalar la APP mencionada, realizamos un backup de los ficheros “nuevos” por si tuviéramos problemas. Luego copiamos nuestro “databases” antiguo que contiene nuestras sincronizaciones con Gmail, Wordpres, etcétera…y volvemos a tener operativo nuestra APP OTP.



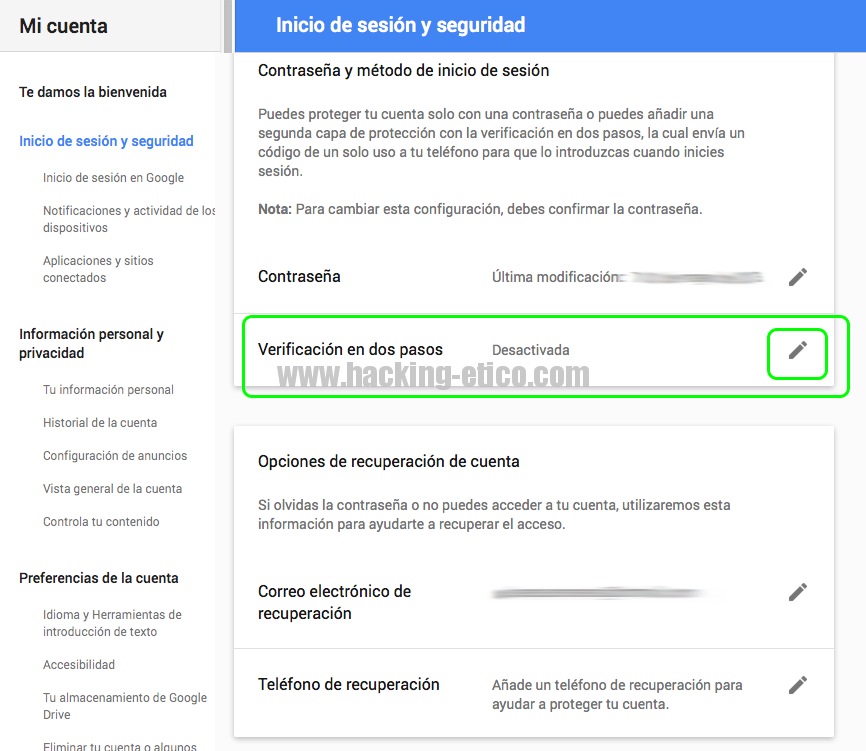
**Actualización 26/11/2015:** **En la versión 2.49 de la aplicación este sistema para “salvar” tus Códigos, no funciona ya que da FC (Forzar Cierre) pero instalando una apk con la 2.44 y realizando el proceso, no hay problema. Se puede actualizar luego.**

Bien, retomando el tema, podemos utilizar tanto aplicaciones OTP o podemos utilizar complementos que envían una clave temporal a nuestro correo. Esto es interesante sino queremos depender de nuestra table o Smartphone a la hora de visualizar las keys temporales. Al correo podemos acceder desde cualquier sitio. Hay que tener en cuenta que si tenemos Gmail con autenticación OTP tenemos que tener otro sistema con el que “comparar” la clave temporal. Es decir, no usemos el mismo correo que está protegido con OTP para que el plugin o complemento que nos mande ahí la key temporal. Sería absurdo.

Evidentemente este método deja un vector de ataque abierto, y es que si el “Correo B” no está protegido con OTP, sería más fácil su ataque que es lo que estamos intentado evitar. Aún así, estamos poniendo ya una traba más al proceso de captura de credenciales.

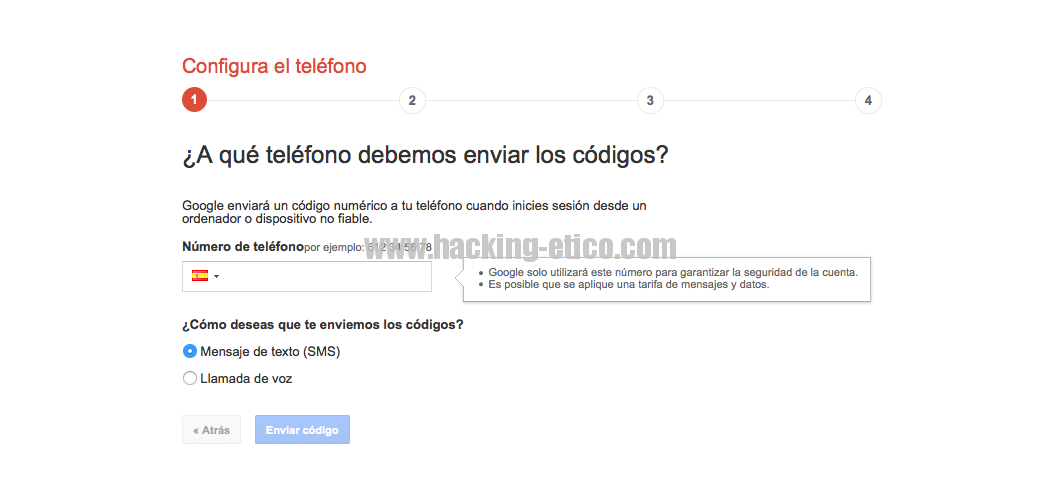
El servicio OTP está poco extendido, es bastante llamativo este aspecto puesto que no es difícil de implementar y da un extra de seguridad muy interesante. Los servicios más conocidos que se puede implementar por ejemplo, son Gmail o WordPress.

Si queremos activarlo en Gmail, debemos irnos a https://myaccount.google.com/security



Veremos una pantalla similar, basta con dar en el icono remarcado en verde para pasar a la siguiente pantalla.



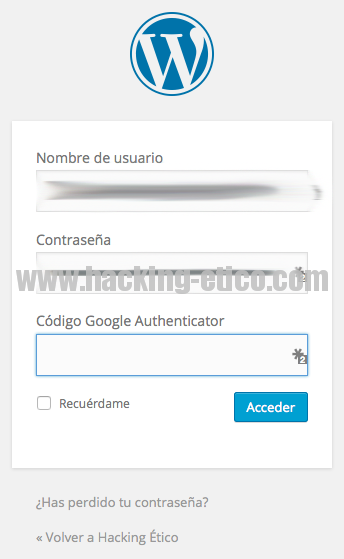
Iniciamos la configuración y veremos una pantalla con una serie de pasos sumamente sencillos. Basta con seguir esto y tendremos activado nuestro sistema OTP. En WordPress tenemos plugins que hacen el trabajo OTP bastante efectivo. Tenemos el plugin “Google Authenticator” que es bastante fácil de usar. Hay otros menos conocidos que igualmente realizan el trabajo pero son más loables a carecer de actualizaciones y de contener problemas de sincronización.

De igual forma, podemos desarrollar nuestro propio plugin OTP como hemos desarrollado en Hacking Ético para la gestión interna. Pero esto ya forma parte de programación WP.

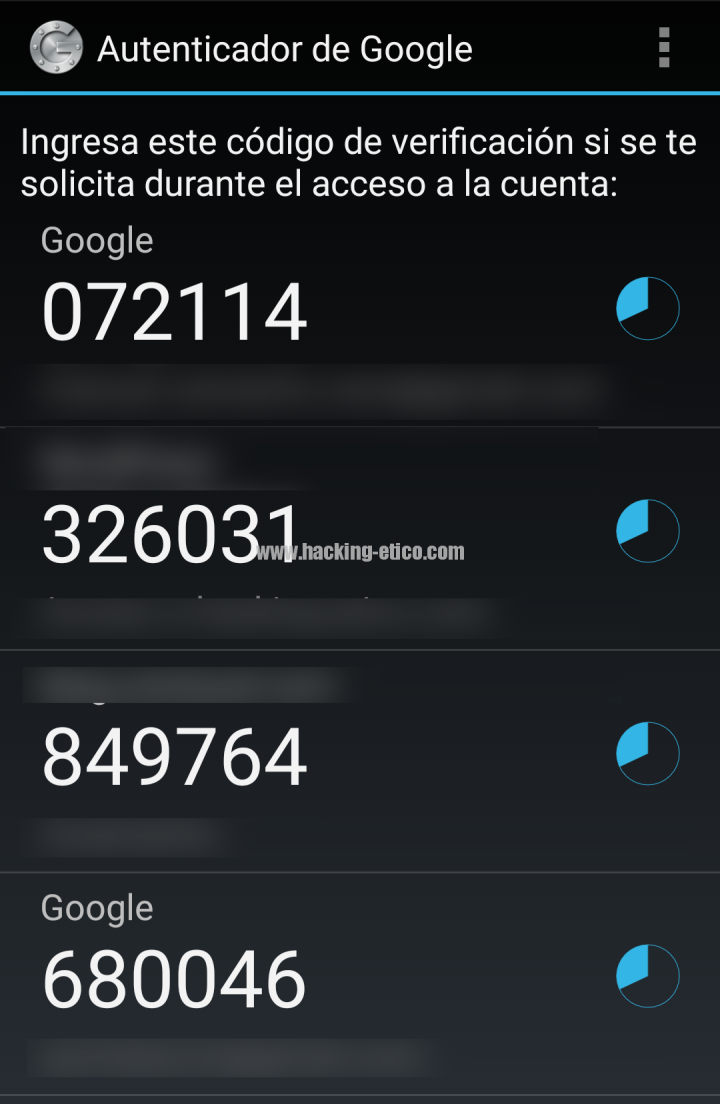
Al instalar Google Authenticator, el plugin, veremos algo así en Ajustes/nombreusuario:



Para completar el proceso, en nuestro Android tenemos que instalar la APP Google Authenticator. A la hora de configurarla nos pedirá o el “Secreto” o el QR Code que contiene el secreto para “sincronizar” la APP con el Plugin WP.

Pantalla de login que veríamos con el Plugin GAuth activado.

A partir de ese momento, cada minuto se generará una key temporal que si logueamos en WP, tendremos que introducir para tener total acceso al Login. Desde ese momento, podremos tener infinidad de ataques de fuerza bruta pero reduciremos enormemente su efectividad, ganando muchísimo tiempo, que es lo importante.

Muestra de ejemplo de la APP Google Authenticator

Con esto, otorgaremos a nuestro WordPress y/o Gmail un extra muy importante de seguridad. Al menos, pese a que esto no es infranqueable, si nuestro sitio se pone a tiro para un atacante, este posiblemente evite “lidiar” con un WordPress que se haya preocupado por ponerlo difícil e irá en la búsqueda de blogs más vulnerables.

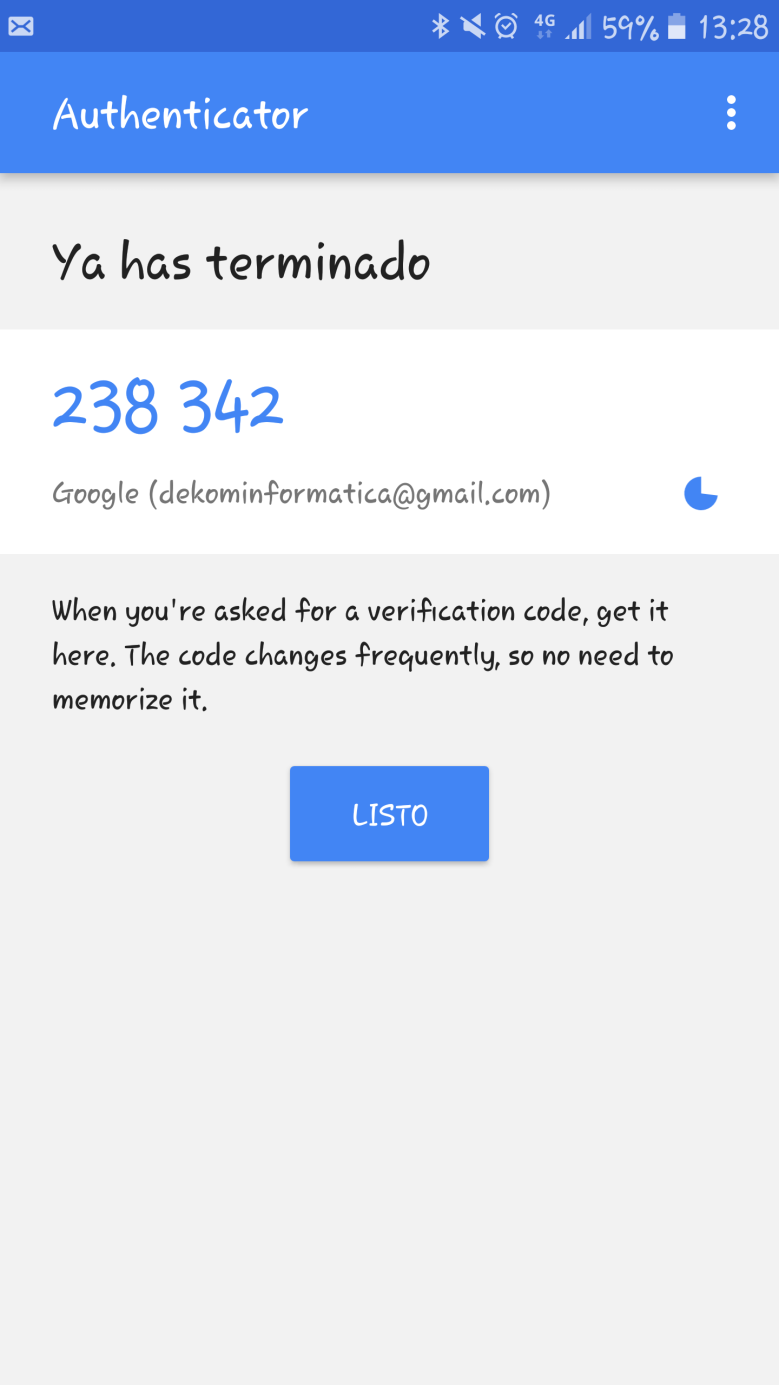
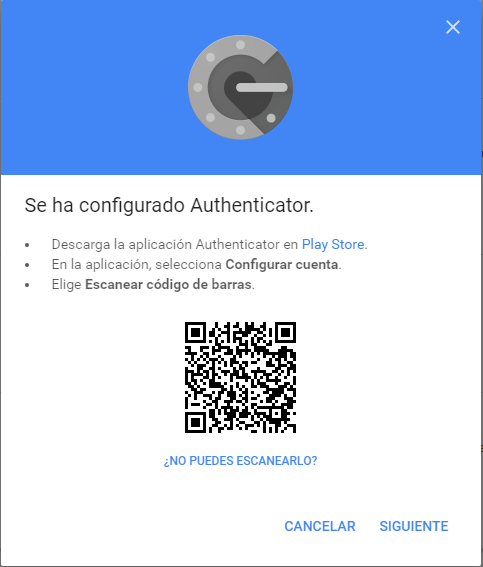
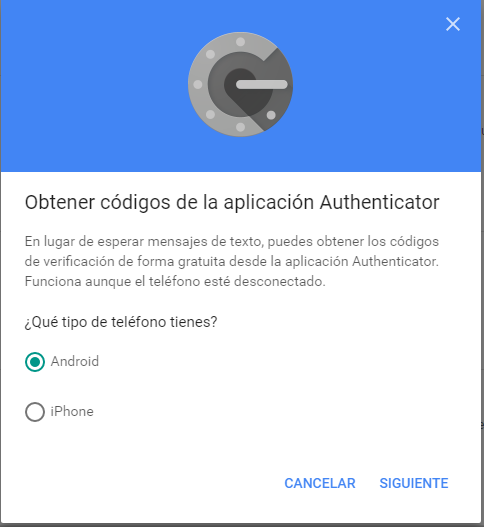
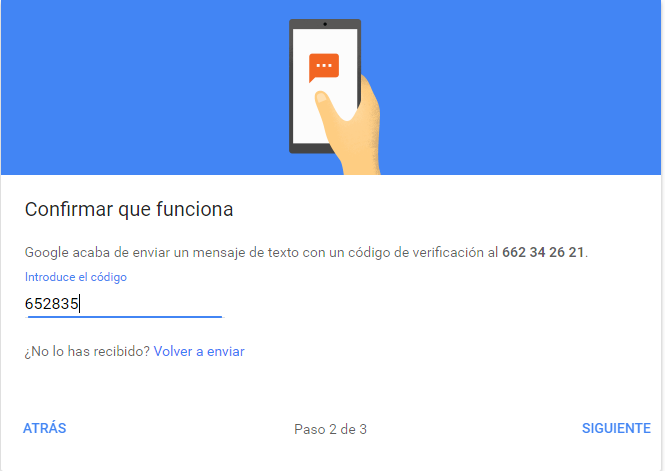
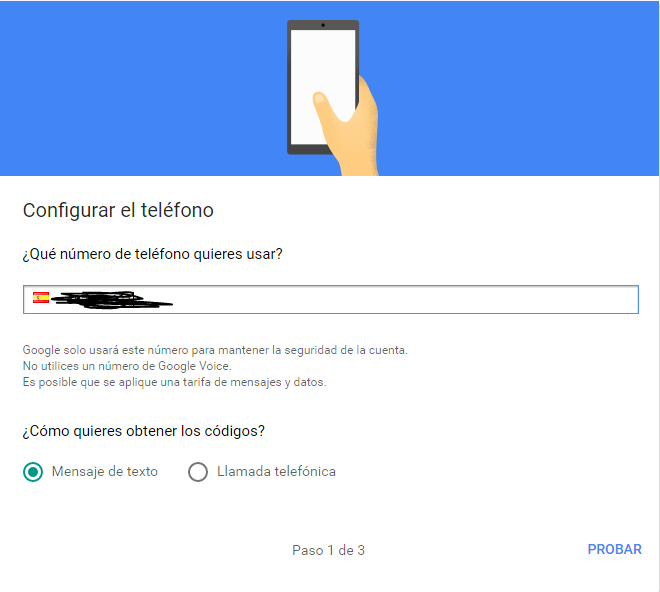
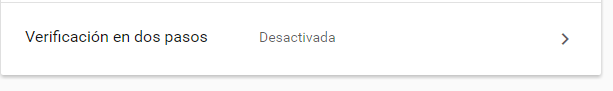
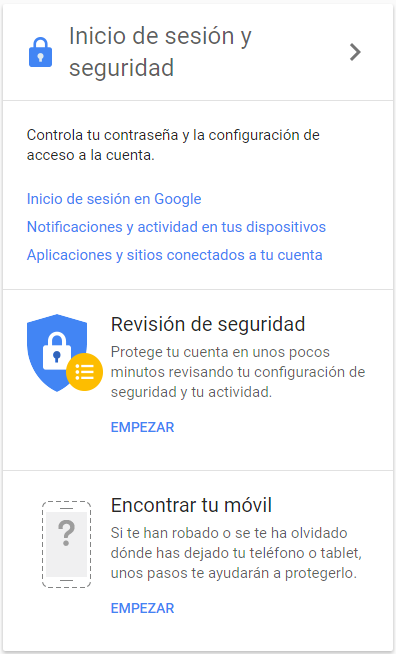
Eso es todo amigos, pese a que no es un tema técnico, si que os puede resultar interesante como medida de seguridad, tan importante hoy en día.

Un saludo!!

**@ManoloGaritmo**

Preguntas:

1.- Realiza un tutorial para activar el servicio OTP en Gmail con tu cuenta de correo.



2.- ¿Qué tiene que ver Google authenticator con Word Press? ¿Cómo se pueden relacionar ambos?

Las dos son aplicaciones que generan códigos siguiendo un patrón, lo cual crea un sistema de seguridad más difícil de descifrar, ya que tendrían que averiguar el patrón y descifrar esos códigos

3.- ¿Google Authenticator es susceptible de sufrir un ataque de fuerza bruta?

Sí, solo que sería un trabajo muy costoso por que tendrían que averiguar el patrón y descifrarlo para saber cual sería el siguiente número

[**Diez consejos para proteger tu correo electrónico**](http://www.muyinteresante.es/tecnologia/articulo/diez-consejos-para-proteger-tu-correo-electronico)

El correo electrónico es una de las vías más frecuentes de entrada de [**virus**](http://www.muyinteresante.es/tag/virus) a nuestros ordenadores. Por este motivo, la compañía de soluciones de software de seguridad Eset ha propuesto un decálogo de buenas prácticas que nos permitirán **protegernos contra el robo de contraseñas, los timos y las infecciones de nuestros equipos**.  
  
**1.** No ejecutar los archivos adjuntos que provengan de remitentes desconocidos. Pon un ejemplo de un adjunto enviado con un email que era un virus, un caso real.

Un correo electrónico, muy común por Navidades, que te invita a abrir una felicitación pero al abrir instala un virus

**2.** De la misma forma, evitar hacer clic en los enlaces incrustados en los correos que provienen de desconocidos o direcciones no confiables. Busca un ejemplo de un enlace incrustado en un enlace que parece real y no lo es.

Cuando descargar programas sin mirar nada sueles aplicar en el buscador o barras o enlaces engañosos por ejemplo: www.google.es/google-

**3.** Los bancos nunca piden información confidencial por e-mail. Un engaño muy frecuente es el *phishing*, que consiste en falsificar la web del banco y redireccionar allí al usuario a través de un enlace. De esta forma pueden hacerse con los datos de identificación del usuario y acceder a su cuenta bancaria. Busca el último twitt sobre la última campaña de phising que se está realizando en España. ¿A qué entidad intentan reemplazar?¿Tienes una foto del phising utilizado?¿Cuál ha sido el último método phising utilizado con los usuarios de iphone para que introdujeran su usuario y contraseña? Busca una foto con el mensaje mandado.

**4.** Habilitar el filtro anti-spam. Haz un tutorial sobre cómo activar el filtro anti-spam en un cliente de correo( Outlook  o Thunderbird) electrónico que configures tu cuenta en una máquina virtual.

[..\..\..\..\SMR1\SMR117\Aplicaciones Ofimaticas\AO\EJERCICIOS\T3-MAIL\_Ac2\_seguridadfiltros\T3\_mail\_Ac2\_Carlos\_Labrador\_Nuria\_Gutierrez.doc](../../../../SMR1/SMR117/Aplicaciones%20Ofimaticas/AO/EJERCICIOS/T3-MAIL_Ac2_seguridadfiltros/T3_mail_Ac2_Carlos_Labrador_Nuria_Gutierrez.doc)

**5.** Utilizar diferentes cuentas de correo. Por ejemplo, es recomendable usar una cuenta exclusivamente para recibir correos con poca importancia, avisos comerciales, mails de listas de correo masivas, etc. Busca dos lugares en internet que te proporcionen un correo durante un espacio corto de tiempo.

Melt mail

**6.** Utilizar **contraseñas seguras**, es decir, que tengan diez o más caracteres e incluyan mayúsculas, minúsculas, números y caracteres especiales. Además es recomendable usar una cuenta por cada servicio. Pon ejemplo de tres contraseñas seguras. Busca 2 sitios en internet, uno que  genere contraseñas seguras y otro que compruebe la seguridad de tu contraseña.



**7.** Evitar acceder al correo electrónico desde equipos públicos. ¿Por qué?

Por que asi evitas que tu contraseña quede guardada o te vean

**8.** Usar con precaución las redes Wi-Fi públicas, puede haber alguien capturando las contraseñas de los usuarios. Explica cómo lo hacen.

Se utilizan programas que te muestran las contraseñas y luego solo hay que descrifrarlas

**9.** A la hora de enviar un mensaje a muchos contactos, utilizar el envío en copia oculta (CCO), de esta forma se protegen las direcciones de los destinatarios. Explica por qué ésta es una buena costumbre.

Asi el resto de destinatarios no ven a quien ha sido enviado el correo

**10.** El mejor aliado de su seguridad cibernética es uno mismo. Es recomendable estar actualizado en materia de seguridad informática.¿cómo puedes estar actualizado en materia de seguridad informática? Da un ejemplo de una página web, una cuenta de twitter y un rss.

EL lado del mal de Chema Alonso y sus libros es una buena forma de estar informado de las nuevas opciones de seguridad informática que van saliendo

 Victoria Gonzalez