

Adios al Phishing

Con las nuevas tendencias globales de comunicacion, la ocurrencia de phishing puede dispararse. Hemos elaborado una guía útil sobre cómo reducir y detener los correos electrónicos de phishing.

Habilitar DKIM y SPF

DKIM (DomainKeys Identified Mail): Es un poderoso recurso presentado en cPanel en 11,32. Esta herramienta va a firmar el correo electrónico con una firma digital que demanda la responsabilidad de los correos electrónicos. Esto le da la capacidad para que los usuarios y a los programas de distinguir entre los correos legítimos y correo electrónico potencialmente falsificados.

SPF (Sender Policy Framework): Es un sistema electrónico diseñado para comprobar la identidad de las líneas de dominio con la dirección IP. De nuevo, esto minimiza la cantidad de correos electrónicos falsificados.

SpamAssassin y BoxTrapper

SpamAssassin: Es una herramienta de correo electrónico que intenta filtrar el spam de correo electrónico entrante mediante el examen y prueba de las características de spam. Utiliza el filtrado Bayesiano de spam y testeo de red para detectar correo electrónico entrante. Esto resulta en una puntuación global. Si un mensaje entrante alcanza una puntuación predefinida, el mensaje se descarta.

BoxTrapper: Actúa como un filtro de spam de direcciones de correo electrónico. El filtro funciona a través de una verificación de «desafío-respuesta». Cuando se envía un correo a una cuenta que ha permitido BoxTrapper, BoxTrapper envía automáticamente un mensaje de confirmación en respuesta.

Compruebe la dirección URL

Si esperas ir a `example.com` y le solicita introducir su nombre de usuario y contraseña, ver la url en el navegador para asegurarse de que coincide con la que desea ir. Si usted espera ver `example.com`, pero en lugar de ver `31337Hax0r.com`, lo más probable es que esta en el sitio equivocado.

Siguiendo estos sencillos pasos, usted puede minimizar los correos electrónicos de phishing que vienen hacia y desde el servidor.