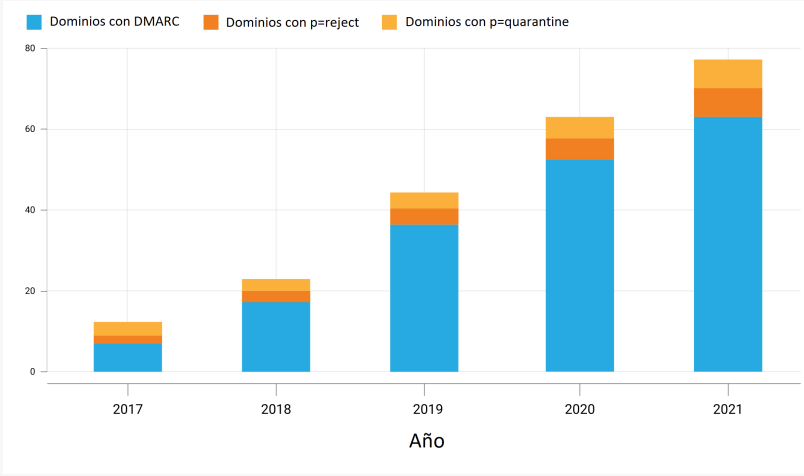
Una investigación de EasyDMARC revela que más de la mitad de las OSAL no están a salvo de los ataques de phishing

Cobertura del protocolo DMARC para la industria de organizaciones sin fines de lucro



El número de dominios con DMARC aumenta progresivamente

MIDDLETOWN, DELAWARE, UNITED STATES, December 8, 2021 /EINPresswire.com/ -- Una investigación de EasyDMARC revela que más de la mitad de las organizaciones sin ánimo de lucro no están a salvo de los ataques de phishing.

Las organizaciones sin ánimo de lucro (OSAL) poseen datos sensibles a los que los hackers apuntan. EasyDMARC puede ayudar a proteger las campañas de recaudación de fondos y a los donantes de las OSAL eliminando la suplantación de dominios de correo electrónico, también conocida como "phishing".

Para las OSAL, defender su causa es sólo la mitad de la historia. El dinero también habla. El éxito de las campañas de donación es fundamental para renovar su presupuesto, tener impacto y aumentar la concienciación. Por ello, la comunicación por correo electrónico es crucial para las OSAL como canal principal para dirigir campañas eficaces de recaudación de fondos y crowdfunding.

En su Informe Global sobre Tecnología para OSAL, Fundraise.org informó de que el 71% de las OSAL envían correos electrónicos a sus colaboradores al menos trimestralmente. Las actualizaciones por correo electrónico se encuentran entre las tres herramientas de comunicación y recaudación de fondos más eficaces, junto con su sitio web y las redes sociales. Por desgracia, el envío de correos electrónicos es también el lugar donde los ciberdelincuentes hacen más daño a las OSAL: justo en la libreta de direcciones de sus donantes.

En su investigación sobre el sector de las OSAL, EasyDMARC analizó los 2000 principales

dominios del sector sin ánimo de lucro y encontró resultados igualmente preocupantes. Aproximadamente el 40% de las 2000 principales organizaciones sin ánimo de lucro mencionadas son usuarias de DMARC, lo que significa que el resto de las OSAL necesita adoptar e implementar DMARC para mantener a sus clientes y empleados a salvo de los ataques de phishing. El siguiente gráfico muestra las políticas durante los últimos 5 años y un aumento en la adopción general de DMARC desde 2017 hasta 2021. Hay un aumento gradual en el número de dominios con DMARC configurado con políticas "p=reject" o "p=quarantine".

El número de dominios con DMARC aumenta progresivamente

EasyDMARC descubrió que el 57% de las OSAL carecían de las políticas DMARC diseñadas para bloquear el uso no autorizado de sus dominios de correo electrónico. Esto significa que los ciberdelincuentes pueden generar direcciones de correo electrónico falsas en nombre de estas organizaciones para llevar a cabo ataques de ingeniería social conocidos como "phishing".

Las OSAL suelen manejar grandes listas, a veces sensibles, de miembros, simpatizantes, activistas y benefactores. La combinación de datos personales, oportunidades de pago por donaciones y el contexto emocional de la labor benéfica proporciona un terreno ventajoso para que los hackers lleven a cabo estafas de ingeniería social, phishing y compromiso del correo electrónico comercial. Para empeorar las cosas, la NTEN informó en su Informe sobre el estado de la ciberseguridad en las organizaciones sin ánimo de lucro que el 68,2% de las OSAL no tienen procedimientos y políticas para responder a un ciberataque.

Por lo tanto, para las organizaciones sin ánimo de lucro es vital empezar a proteger su entorno de correo electrónico. No sólo para proteger la eficacia de sus campañas de recaudación de fondos, sino también para asegurar a sus miembros, donantes y su propia reputación dentro del sector no lucrativo. Para ayudar a las OSAL a mantener la confianza de su comunidad, EasyDMARC proporciona herramientas flexibles y fáciles de implementar que las mantendrán a salvo de los ciberdelincuentes.

El servicio es gratuito para las pequeñas organizaciones, con planes adaptables para las OSAL, y puede implantarse en menos de 24 horas. EasyDMARC permite a las organizaciones sin ánimo de lucro asegurar su ecosistema de correo electrónico en torno a 4 registros de correo electrónico esenciales: DMARC, SPF, DKIM, BIMI. Una vez establecidas, estas protecciones garantizan que los hackers no puedan suplantar el dominio de correo electrónico de la organización.

Una ventaja secundaria de EasyDMARC para las OSAL es que es mucho menos probable que sus correos electrónicos acaben en la carpeta de correo no deseado de sus destinatarios: donantes, suscriptores de boletines o socios. Como explica Gerasim Hovhannisyan, CEO de EasyDMARC: "Una vez implantado el DMARC en sus dominios de correo electrónico, las OSAL pueden llegar a sus simpatizantes y al público en general de forma más fácil y directa, sin que los filtros de spam los desbaraten. Estamos encantados de ayudarles a aumentar la eficacia de su comunicación,

para que su voz sea escuchada por más personas, recaudando más fondos para servir a su causa."

Con una seguridad del correo electrónico notablemente mejorada gracias a haber asegurado sus registros DMARC con EasyDMARC, las organizaciones sin ánimo de lucro pueden volver a centrarse en lo que mejor saben hacer: llegar, informar e implicar a sus miembros para mejorar la vida de su comunidad y de la sociedad.

Sobre EasyDMARC

EasyDMARC ofrece soluciones para que las empresas puedan garantizar la seguridad de su correo electrónico y marketing directo en internet, de forma rápida y sin necesidad de conocimientos especializados. Las soluciones de EasyDMARC protegen a las empresas contra la fuga de datos, las pérdidas financieras, los ataques de suplantación de identidad por correo electrónico y evitan el uso no autorizado de su nombre de dominio y direcciones de correo electrónico. Más información disponible en https://easydmarc.com/.

Fuentes

https://www.nten.org/wp-content/uploads/2018/11/Cybersecurityreport2018NTEN.pdf

https://www.funraise.org/techreport/infographics

Gerasim Hovhannisyan
EasyDMARC, Inc.
+1 888-563-5277
gerasim@easydmarc.us

Visit us on social media:

Facebook

Twitter

LinkedIn
