proofpoint

PROOFPOINT EMAIL FRAUD DEFENSE

EL CORREO ELECTRÓNICO ES EL PRINCIPAL VECTOR DE RIESGO DE LAS EMPRESAS

- El phishing con arpón es eficaz: el 30 % de los destinatarios abren los mensajes de phishing y el 12 % hace clic en los archivos adjuntos.[1]
- La vulneración de correo electrónico de empresas (BEC), o estafa de correo electrónico de impostores, ha costado más de 3100 millones de dólares a las empresas desde enero de 2015.[2]
- El phishing de arpón se puede prevenir: el 80 % del correo electrónico de impostores falsifican dominios de confianza y se pueden bloquear antes de que lleguen a la bandeja de entrada.[3]

CARACTERÍSTICAS

- Visibilidad granular en todo su ecosistema de correo electrónico
- Identificación en tiempo real de los mensajes que no pasen la autenticación
- Configuración dinámica de excepciones, alertas y reglas en la puerta de enlace de Proofpoint Email Protection

VENTAJAS

- Bloquee los mensajes de BEC o de impostores que falsifiquen dominios de confianza, tanto los suyos como los de sus socios, antes de que lleguen a sus empleados y clientes
- Bloquee las infecciones de ransomware, el fraude de transferencias monetarias y las brechas de formularios W-2
- Disipe las inquietudes del consejo directivo mediante la prevención del robo de identidad y la mitigación de la exposición a riesgos

ELIMINACIÓN EL IMPACTO DEL FRAUDE POR CORREO ELECTRÓNICO

El fraude por correo electrónico es abundante: las vulneraciones de correo electrónico de empresas (BEC) están costando miles de millones de dólares a las empresas y el phishing dirigido a los consumidores ha alcanzado un máximo histórico. La mayoría de esos ataques de correo electrónico se puede prevenir.

Al aprovechar el poder de la autenticación del correo electrónico (SPF, DKIM y DMARC), Proofpoint Email Fraud Defense protege a su organización de todos los ataques de phishing (incluyendo un 80 % de los mensajes de impostores) que falsifican dominios de confianza.

Al tener visibilidad respecto a quién está enviando mensajes en toda la empresa, podrá autorizar a todos los remitentes legítimos y bloquear los mensajes fraudulentos antes de que lleguen a sus empleados, socios comerciales y clientes.

Al implementar Email Fraud Defense con nuestras otras defensas, usted podrá anular toda una clase de fraude por correo electrónico de impostores. Emplee nuestras soluciones para:

- Detener el ransomware basado en correo electrónico
- Evitar ataques de transferencia monetaria de director ejecutivo o financiero, y de estafa con formularios W-2
- Bloquear el correo electrónico con suplantación de identidades de empresa y marca antes de que lleguen a sus empleados y clientes

VISIBILIDAD GRANULAR

Comprenda quiénes están enviando correo electrónico en toda su empresa

Email Fraud Defense le ayuda a comprender sus datos de autenticación del correo electrónico mediante la interfaz de informe DMARC (Domain-based Message Authentication Reporting & Conformance) que proporciona los resultados de la autenticación de todo el tráfico de correo electrónico que entra en y sale de su organización. Interpretamos los datos mediante algoritmos automatizados que hacen distinción entre las anomalías y los problemas que necesiten atención.

Con Email Fraud Defense podrá:

- Vigilar todos los mensajes de correo electrónico (entrantes y salientes) de sus dominios y de los de terceros
- Distinguir de forma precisa entre los mensajes de correo electrónico legítimos y los fraudulentos que no pasen la autenticación
- Comprender los motivos que haya detrás de cada error de autenticación

1 "2016 Data Breach Investigations Report" [Informe de investigación de brechas de datos de 2016], abril de 2016
2 "Business E-Mail Compromise: The 3.1 Billion Dollar Scam" [Vulneración de correo electrónico de empresas: La estafa de 3100 millones de dólares], junio de 2016.
3 Proofpoint. "Impostor Email Threats" [Amenazas de correo electrónico de impostores], marzo de 2016

BLOQUEE LAS AMENAZAS DE CORREO ELECTRÓNICO Y ELIMINE LOS RIESGOS

Implemente una política de rechazo de DMARC sin el riesgo de que haya falsos positivos.

Si se activa una política de rechazo de DMARC, esta bloqueará todos los mensajes de correo electrónico procedentes de direcciones IP que no tengan su autorización para enviar mensajes desde su dominio. Sin embargo, la implementación de DMARC también podría ocasionar que se bloqueen mensajes entrantes legítimos. Email Fraud Defense es la única solución de autenticación del correo electrónico que le brinda la implementación total de DMARC con más rapidez y con menos riesgo.

Con Email Fraud Defense podrá:

- Recibir instrucciones claras de flujo de trabajo para acciones de políticas de autenticación de correo electrónico
- Configurar excepciones, alertas y reglas en la puerta de enlace de Proofpoint Email Protection para cualquier escenario de remitente
- Indicar a la puerta de enlace de Proofpoint Email Protection que bloquee las amenazas antes de que lleguen a las bandejas de entrada de sus empleados y consumidores

RECIBA SOPORTE

Nuestro equipo global de expertos en correo electrónico está a su disposición para ayudarle.

Es difícil lograr que sus flujos de correo legítimo (así como los de sus proveedores y socios) se autentiquen de forma correcta sin recibir soporte. Nuestro equipo de servicios profesionales elabora planes personalizados de implementación de proyectos y desarrolla una evaluación de riesgos exhaustiva, al mismo tiempo que brinda una implementación DMARC libre de problemas y la administración constante.

Nosotros haremos lo siguiente:

- Actuar como extensión dedicada de sus equipos internos, analizando los datos de amenazas de correo electrónico para ayudarle a comprender la naturaleza de los ataques identificados
- Brindar soporte continuo a media que evolucionen sus prácticas de correo electrónico empresarial
- Ofrecer monitorización continua para optimizar su implementación DMARC