CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

AUTENTICACIÓN DE EMAIL

Su compañía puede ayudar a prevenir las estafas de phishing usando tecnología de autenticación de email.

Con la tecnología de autenticación de email a un estafador le será mucho más difícil enviar emails de phishing que parezcan ser enviados desde su compañía.

LO QUE HAY QUE SABER —

Algunos proveedores de servicios de alojamiento web le permiten configurar el email comercial de su negocio usando su nombre de dominio (que es lo que puede pensar como el nombre de su sitio web). Su nombre de dominio podría ser algo como sunegocio.com. Y su domicilio de email podría ser algo como nombre@sunegocio.com. Si no tiene un sistema de autenticación de email, los estafadores pueden apropiarse de ese nombre de dominio y enviar emails que parecen ser enviados desde su negocio. Si el email de su negocio usa el nombre de dominio de su compañía, asegúrese de que su servicio de alojamiento web tenga las siguientes tres herramientas de autenticación de email:

La tecnología SFP (Sender Policy Framework)

les indica a los otros servidores cuáles son los servidores que tienen permitido enviar emails usando el nombre de dominio de su negocio. De modo que cuando usted envía un email desde nombre@sunegocio.com, el servidor receptor puede confirmar si el servidor emisor está en una lista aprobada. Si está en la lista, el servidor receptor deja entrar el email. Si no lo encuentra en la lista, el email puede marcarse como sospechoso.

La tecnología DKIM (Domain Keys Identified Mail)

coloca una firma digital en el correo saliente para que los servidores puedan verificar que un email de su dominio fue enviado verdaderamente desde los servidores de su organización y no fue manipulado en tránsito.

DMARC (Domain Message Authentication, Reporting & Conformance)

es la tercera herramienta esencial para la autenticación de email es el sistema. Las herramientas SPF y DKIM verifican el domicilio que usa el servidor "detrás de escena". El sistema DMARC verifica que este domicilio corresponda al domicilio del remitente, o "de", que usted ve. También le informa a otros servidores cómo actuar cuando reciben un email que parece provenir de su dominio pero el servidor receptor tiene motivos para identificarlo como sospechoso (según lo que indica SPF o DKIM). Usted puede establecer que otros servidores rechacen el email, lo marquen como spam o que no tomen ninguna acción. También puede establecer la herramienta de autenticación de email DMARC para que lo notifiquen cuando suceda.

Para configurar estas herramientas de manera que funcionen tal como se desea y no bloqueen los mensajes de correo electrónico legítimos hay que tener cierto nivel de experiencia técnica. Asegúrese de que su proveedor de servicio de alojamiento web pueda configurarlas en caso de que usted no tenga los conocimientos técnicos necesarios. Si el proveedor no puede hacerlo, o si esto no está incluido en su contrato de servicio, considere buscar otro proveedor.

CIBERSEGURIDAD PARA
PEQUEÑOS NEGOCIOS

QUÉ HACER SI SU EMAIL SUFRE UN
ATAQUE DE SUPLANTACIÓN

Las herramientas de autenticación de email ayudan a evitar que alguien use el email de su negocio en estafas phishing porque le notifican si alguien manipula el email de su compañía. Si recibe esa notificación, tome las siguientes medidas:

Repórtelo

Reporte la estafa a las autoridades de seguridad locales, al Centro de Quejas de Delitos en Internet del FBI en ic3.gov, y a la FTC en ftc.gov/queja. También puede reenviar los emails phishing a spam@uce.gov (un domicilio electrónico utilizado por la FTC) y a reportphishing@apwg.org (un domicilio electrónico utilizado por el Grupo de Trabajo Anti-Phishing, que incluye proveedores de servicios de internet, proveedores de productos y servicios de seguridad, instituciones financieras y agencias a cargo del cumplimiento de la ley).

Notifique a sus clientes

Si descubre que hay estafadores que se hacen pasar por su negocio, infórmeselo a sus clientes a la brevedad posible – por correo, email o a través de los medios sociales. Si se comunica con sus clientes por email, envíe un mensaje de correo electrónico sin hipervínculos para que su notificación no parezca una estafa de phishing. Recuérdeles a sus clientes que no compartan ninguna información personal a través del correo electrónico o mensajes de texto. Y si le roban los datos de sus clientes, dígales que visiten RobodeIdentidad.gov para conseguir un plan de acción para recuperarse.

Alerte a su personal

Use esta experiencia para actualizar sus prácticas de seguridad y capacitar a su personal acerca de las amenazas cibernéticas.