Seguridad de Páginas Web

Los sitios web son un territorio con un valor incalculable:

- Si un criminal cibernético logra acceso a tu sitio web, habría encontrado un lugar gratuito y seguro para implantar malware, correos no deseados, publicidad o suplantación de identidad. ¡Estos criminales están constantemente buscando todo tipo de sitio web vulnerable para controlarlo!
- Cualquier persona que quiera atacar a tu organización, puede hacerlo a través de tu sitio web. Pueden intentar adivinar tus credenciales, encontrar tus contraseñas en una lista filtrada de datos por alguna brecha de seguridad, o usar un botnet para sobrecargar tu página web con tráfico (un ataque DDoS o servicio denegado de distribución).
- Los acosadores que usen de blanco tu organización para atacarla pueden encontrar fotos y las direcciones de correo electrónico de la junta, empleados y voluntarios y usar ese contenido para hacer más daño.

¡Afortunadamente, existen formas de protegerse en contra de estos potenciales ataques!

Lista de seguridad para tu sitio web:

- ❏ Certificado SSL (el ícono que parece un candado en la barra del URL)
- ❏ Protege todas las formas con CAPTCHA (Google o hCaptcha) para prevenir comunicaciones no deseados y fraude
- ❏ Permitir la protección gratuita de DDoS de Deflect.Ca, Project Galileo (Cloudfare) o Project Shield (Google) Enable DDoS protection for free from either Deflect.ca, Project Galileo (Cloudflare), or Project Shield (Google)
- ❏ Cualquier persona que necesite acceso al sitio web debe serle provista su propia cuenta con una contraseña única y que no sea fácil de descifrar
- ❏ Usar el sistema de autenticación de dos factores si es posible
- ❏ Usa formularios de contacto en lugar de publicar los correos electrónicos de los empleados
- ❏ Crear un itinerario actualizado y coordinar el recibo de notificaciones
    - ❏ Entrenar y designar a alguien para que actualice la página web
    - ❏ Encender actualizaciones automáticas si es posible

- ❏ Mantener una lista de información esencial del sitio web en un lugar seguro que por los menos dos empleados tengan acceso
    - ❏ La lista debe incluir en donde el dominio web está alojado, un enlace para actualizar el certificado de SSL en caso de que expire y el enlace donde puedes ir a editar el sitio web
    - ❏ Guarda los credenciales del sitio web por separado con un administrador de contraseñas
- ❏ Opcional para privacidad adicional: usar avatars en lugar de las fotos de los empleados y quita los biográficos de empleados