Vérifiez l'authenticité et la fiabilité de l'expéditeur.
En cas de doute, contactez l'expéditeur par téléphone avant de répondre au message reçu par e-mail.

Vérifiez si les messages, qui sollicitent vos données privées, comportent des erreurs de frappe, des fautes d'orthographe ou des expressions inappropriées. En cas de doute, évitez d'y répondre, de cliquer sur les liens hypertextes ou les images qu'ils contiennent et supprimez-les immédiatement.

Contactez le RSSI de l'entreprise dans le cas où le contenu de l'e-mail est douteux et n'y répondez pas. Scannez immédiatement les pièces jointes avec votre solution anti-virus avant de les consulter.

Appliquez les « Bonnes pratiques pour se protéger contre la technique de Phishing: Display Name Impersonation».

Mesures préventives pour vos serveurs de messagerie

Implémentez les techniques « DNS Reverse Lookup », SPF (Sender Policy Framework -RFC 4408), DKIM ADSP (Author Domain Signing Practices -RFC 5617) et DMARC (Domain-based Message Authentication, Reporting, and Conformance – RFC 7489) pour vous permettre de distinguer les domaines des serveurs de messagerie émetteurs suspects.

Appliquez des règles de filtrage rigoureuses pour éviter tout accès d'administration non autorisé à vos serveurs de messageries et maintenez à jour vos solutions anti-virus, pare-feu et vos filtres de messagerie pour réduire le trafic provenant des Spams.

Contrôlez votre trafic « Remote Desktop Protocol (RDP) » et appliquez des règles d'accès rigoureuses .