Online Trust Alliance

TIPS FOR BUSINESES & TAX FILING PROFESSIONALS

Keep your company's and customers' information safe during tax filing season

❑	**Recognize Security and Privacy are not Absolutes and Must Evolve.** Regularly review how you store, manage and secure your data. Encryption is a fundamental requirement and failure to encrypt is frequently being cited as the cause for regulatory action and lawsuits. Test the SSL configuration of your servers monthly. Suggested tools include https://ota.ssllabs.com/ and https://www.htbridge.com/ssl/.
❑	**Know Your Users.** Enforce effective password management policies. Attacks against user credentials, including spear phishing, brute force, sniffing, host-based access and theft of password databases, remain very strong attack vectors warranting the use of effective password management controls. Adopt multi-factor authentication (e.g. smartcard and PINs in addition to a password) for access to administratively privileged accounts.
❑	**Help Consumers; Curb Fraudulent Email.** Require email authentication on mail servers to help detect malicious email, spear phishing and spoofed email. All organizations should authenticate outbound and inbound email with SPF and DKIM, and adopt a DMARC with reject or quarantine policies. https://otalliance.org/eauth.
❑	**Only Allow Trusted Devices.** Permit only authorized wireless devices to connect to your network, encrypt the traffic of wireless communications and devices such as routers, printers, point of sale terminals and credit card readers. Keep all "guest" network access on separate servers and employ strong encryption on access devices including personal devices and phones used by employees.
❑	**Stop Cyber Eavesdropping.** Implement Always On Secure Socket Layer (AOSSL) for all servers requiring log on authentication and data collection. AOSSL helps prevent sniffing of data being transmitted between client devices, wireless access points and intermediaries.
❑	**Know Who Your Sites Are.** Secure your WHOIS records and review server certificates for vulnerabilities to assess the risk of your domains being hijacked. Attackers have targeted "Domain Validated" (DV) SSL certificates to impersonate websites and defraud consumers. Upgrade to "Organizationally Validated" (OV) or "Extended Validation" SSL (EVSSL) certificates. EVSSL certificates offer the highest level of authentication, providing assurance that the site owner is who they purport to be by presenting the user a green trust indicator. https://otalliance.org/SSL and https://cabforum.org/about-ev-ssl/.
❑	**Security & Privacy Is Beyond Your Walls.** As more businesses rely on cloud services, organizations must complete risk assessment of their vendors on an ongoing basis. Assessments should review e-providers' security and data privacy practices, confirming alignment to your standards, regulatory requirements and policies.
❑	**Being Prepared Is Not Just For Boy Scouts**. Test and continually refine a data breach response plan. Regularly review and improve the plan based upon changes in your organization's information technology, data collection and security posture. https://otalliance.org/Breach.

