Cyber Security Checklist

Adhering to a Cyber Security Policy is crucial to protecting all shows from cyber phishing risks and to safeguard company funds. The prevalence of cyber-attacks is on the rise and extra diligence is now required.

Here are 10 easy points to help protect show's financial assets in today's cyber risk environment.

1. **Verify the Caller's Identity:**

If inbound calls are unsolicited, ask for the caller's name, organization, and contact information. However, keep in mind that scammers can provide fake information.

2. **Do Not Share Personal or Show Information:**

Avoid sharing personal or financial information over the phone or email, especially if you did not initiate the call or email. Legitimate organizations will not ask for sensitive information such as passwords or Social Security numbers over the phone.

3. **Hang Up:**

If you are unsure about the call, it's okay to hang up. You can also delete the email. You can then independently verify the author's / caller's identity through official channels.

4. **Call the Official Number:**

Use official contact information obtained from the organization's official website or other reliable sources to call them back. Do not use the phone number provided by the caller.

5. **Secure Financial Transactions:**

Please establish a strict verification process for any changes to payment details or financial transactions. Where appropriate, use secure and encrypted payment gateways for all financial transactions.

6. **Never click on any links in unsolicited or unknown emails**

Always enquire with the official organisation about the legitimacy of their enquiry. Right mouse click on the author's email to reveal the originating email address (if hidden) and see if it is from the official company email address. Often threat actors disguise the originating email address to avoid suspicion.

7. **Show Volunteer / Employee Training and Awareness:**

Conduct regular training sessions for relevant volunteers / employees to educate them on phishing risks. Raise awareness about the latest phishing techniques and tactics. Test knowledge where appropriate to ensure they can identify and report suspicious emails.

8. **Use Multi-Factor Authentication (MFA):**

Implement MFA for all systems and applications where appropriate, especially those related to financial transactions. Ensure that relevant volunteers/employees use strong, unique passwords in conjunction with MFA.

9. **Email Filtering and Authentication:**

Employ advanced email filtering systems to detect and block phishing emails. Implement email authentication protocols such as DMARC (Domain-based Message Authentication, Reporting, and Conformance) to prevent email spoofing.

10. **Regular Software Updates and Patching:**

Ensure that all software, including operating systems, antivirus, and anti-malware solutions, are regularly updated with the latest security patches.

This document was prepared with the assistance of AgShow NSW's Insurance Broker, PSC Insurance. If you have any queries to contact us at asc.admin@ascofnsw.org.au

Cyber Security Checklist published February 2024