Sony Music Content Security Guidelines for Recording Artists

Intended Use:
The following are guidelines that Sony Music Entertainment (SME) has developed over time to assist Recording Artists and their teams to devise and implement an effective security plan to secure SME pre-release recordings. The general guidelines and considerations below are provided for informational purposes only and without warranty, express, implied or otherwise, regarding the accuracy or completeness of the information. SME accepts no responsibility or liability for the consequences of any actions taken in reliance on the information provided herein.

General Guidelines

It is recommended that Recording Artists establish and communicate a security plan prior to recording to ensure all the relevant parties are aware of the security requirements at the outset of a project. Security is only as strong as its weakest link, so it is important that all parties fully understand and follow the security plan.

The following are recommendations that Recording Artists should consider as part of any action plan.

- As a general rule of thumb, personnel who handle pre-release recordings should use secure delivery methods to transmit recordings to, from, and within the artist camp
    - It is recommended that recordings be delivered on physically encrypted storage devices or using an SME-approved secure digital delivery solution such as SME's Secure File Transfer System (SFTS) and PreAmp
    - Avoid using public email, file sharing, or file hosting services to send, receive, or store SME recordings
    - In the event recordings are transmitted via email, all Sent and Received messages used to transmit recordings should be immediately and permanently deleted upon delivery

- Recordings should be stored in a secure, offline location inaccessible via the Internet (i.e. if the recordings are inaccessible via the Internet, it will not be susceptible to online phishing and hacking attempts)
    - Encrypt external storage devices used to store recordings
    - Password protect recordings using programs such as WinRar or WinZip and communicate passwords separately via text message or over the phone

- Personnel who work with recordings should avoid sharing account credentials with other individuals
- Care should be taken at all times to restrict access to recordings and to limit sharing to only authorized personnel
    - Unsolicited requests for music received via email should be confirmed over the phone prior to sending music
    - Recording sessions should take place in a secured location without Internet connectivity
    - Where possible, recordings should be recorded in-person and outside producers should be encouraged to appear in-person to preview and submit recordings

- Artists should hold listening sessions at a secured, controlled environment. The host of the listening session should enforce a strict no-cell-phone policy and remind all attendees in advance of the meeting of the policy.
- The number of copies used to promote a release should be kept to a minimum

Preventative measures to protect against phishing or malware attacks

- Use up-to-date applications, operating systems and anti-virus software on mobile devices, tablets, and laptops/computers
- Enable two-factor (2FA) or multi-factor (MFA) authentication on all accounts used to transmit and store recordings
- Use different passwords for different accounts to prevent hackers from using compromised credentials to gain access to other accounts. All accounts should utilize strong passwords (i.e. unique passwords that consist of a minimum of 12 characters comprising uppercase letters, lowercase letters, numbers, and special characters). Avoid using previously used passwords and remember to update passwords frequently.
- Be on the lookout for suspicious email (e.g., email containing mistakes in the sender's address, requests that ask you to provide or update your account settings, etc.)
- Phishing email may come in the form of an email chain pretending to be from someone you know. If you are uncertain about the origin of any email, call the sender to confirm the request.
- Avoid clicking on suspicious links or attachments that may contain malware. Run the cursor over a link to see where it actually leads – attackers will often take advantage of spelling mistakes to misdirect you. To confirm that a link is safe to access, scan the link using online malware detection services such as Norton SafeWeb, Virus Total, URLVoid and ScanURL
- Don't use public Wi-Fi access points to access sensitive information and don't ignore invalid security certificate warnings

In the event that you receive a phishing email or notice unusual activity on your account, consider the following response measures to identify potential vulnerabilities

- Check the Security settings to review recent account activity, connected devices, and third-party access to determine if other users and/or devices accessed the account
- Check the Account settings to change your password and password recovery options (e.g., recovery phone, recovery email, security questions) to prevent hackers from bypassing your login credentials
- Check the Account settings to confirm that no additional accounts were granted access to your account without your knowledge (allowed to read and send messages on your behalf)
- Check the Filtering settings to confirm that no filtering rules were added without your knowledge
- Check the Forwarding settings to confirm that no forwarding email addresses were added without your knowledge
- Check the POP/IMAP email settings to confirm that no third-party email clients were granted access to the email account without your knowledge
- Check the Account Settings to enable two-factor authentication or multi-factor authentication on the account (e.g., user account verified with password AND 6-digit code sent via text message)
- Review Sent Items in your accounts to confirm that no files were sent without your knowledge
- Notify your SME representative of any suspicious activity

- SME has resources available to investigate leaks and to help mitigate damages that may result from leaks
- Provide as much detail as possible at your discretion. In general, the more information that is provided, the greater the likelihood of identifying the culprit
    - This may include the account information, email address of a sender, list of compromised titles, examples of phishing or suspicious emails, and the time at which the incident occurred
- SME will review the information and take appropriate steps to prevent phishing and hacking attempts to its network. This may include blocking email addresses from the corporate network to prevent hackers from targeting Sony accounts. In addition, SME may provide such information to the appropriate authorities and law enforcement agencies.
- Lastly, notify associates to make them aware that they may receive fraudulent emails appearing to come from you