PROTECTING YOUR WORK
RIAA Security Best Practices Recommendations

Account Registration:

1. When registering for a new account on a service, avoid using your legal or artist name (or other personal information), business email address, or other email address that you use for transmitting confidential information, as part of the account registration.

Passwords:

2. Use a password manager to manage passwords for your accounts. Also, ensure your password manager has a very complex, random password, and uses multi-factor authentication (MFA). Using a password manager will provide for more secure and different passwords for your accounts, while not requiring you to remember multiple passwords.
3. If you don't use a password manager, at least use a unique, different, and complex password for each site or service on which you have an account and ensure the password does not include personal information.
4. Never share passwords with anyone.
5. Where possible, use MFA for access to your accounts, and use a software authenticator, rather than text, email or phone authentication for the MFA. Consider using USB/NFC enabled security keys for additional security.

Communications (emails, links, texts, social media direct communications, etc.):

6. Check the content / addresses of any communications you receive to see if they are legitimate. In particular, check the content / addresses of any out of character communications you receive for any mistakes / misspellings or unsolicited requests for personal information. If it looks wrong, or doesn't feel right, contact the sender using the information you have for the sender via a separate communication thread (i.e., not through the information contained in that communication), or ignore the communication, and don't click on any links in the message.
7. In expected communications, hover over any link with your cursor to confirm it is taking you where you expect to go before clicking on it. Don't click on the link unless it is taking you where you expect to go. Preferably, visit websites by typing the domain name yourself. Never supply personal information/passwords via email.
8. Regularly, check (a) your email account settings for any auto-forwarding rules, (b) your apps for any third-party app access that may have been added to your account without your knowledge, and (c) your deleted emails and "Sent" folder for any messages sent without your knowledge or consent.

Protecting your work generally:

9. Ensure your computers / internet connected devices are using up to date operating systems, applications, and anti-virus software.
10. Delete any unused applications or software from your devices. Also delete any unused, historical accounts on any services. Only install apps from an authorized app store.
11. Ensure your routers / wifi are password protected (with a complex pw) and avoid using public wifi for sensitive work.
12. If you need to work on a public wifi, use a VPN to further secure your work.

Protecting your work in the cloud:

13. Only use cloud storage that offers security and MFA, with a software authenticator where available. Consider using different cloud storage providers or different cloud storage accounts for different projects.
14. Follow steps 1-5 above to protect the account for your cloud storage.
15. Encrypt files when uploading sensitive files to your cloud storage account and use abbreviated file names to obfuscate the contents of the file.
16. If you need to share your music with others, send links that only permit streaming, not downloading.
17. When available, only share pre-release content using tools that embed a watermark.
18. Ensure those links are password protected, have expiration dates, and only available for the intended recipient.
19. After the recipient has received the file, disable the link and/or remove or rename the file.
20. Never give someone access to your entire cloud account. Only share relevant files with select individuals.

Glossary / Examples of Services

Complex password and password managers:

- A complex password should be least 8-15 or more characters in length, use no common names or dictionary words or account names, have no sequences of more than 4 digits in a row, and include a least one character from at least 3 of the following categories: upper case letter, lower case letter, digits, and a special characters. An example of a complex password would be EK.xaCqNKf$9l?FV.
- Some password manager services that have been recommended include, among others: Keeper, Dashline, LastPass, LogmeOnce, KeePass and Password Boss.

Software authenticators:

- Some software authenticators that help provide multifactor authentication that have been recommended in 2021 include, among others: Authy, Google Authenticator, and Microsoft Authenticator.

USB/NFC (near field communication) enabled security keys*:*

- These are hardware based multifactor authentication products/services to further secure your valuable, online accounts.
- Some USB/NFC enabled security products/services that have been recommended in 2021 include, among others: YubiKey 5C NFC, Yubico Yubikey 5 NFC, Thetis Fido U2F Security Key and Google Titan Security Keys

Cloud storage solutions:

- Some cloud storage solutions that have been recommended in 2021 include, among others: iCloud, Google Drive, and One Drive.

VPN Services:

- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted.
- Some VPN services that have been recommended in 2021 include, among others:
  - For your computer: NordVPN, Private Internet Access VPN, Surfshark, & CyberGhost
  - For your iphone: ProtonVPN, IVPN, NordVPN, Private Internet Access VPN, and Surfshark
  - For your android phone: ProtonVPN, NordVPN, Private Internet Access VPN, Surfshark and CyberGhost

This list of Recommendations was created by the RIAA, shared with the Recording Academy Producers & Engineers Wing, and reviewed by two Chief IT officers prior to posting.