CAPLAW enews brief

Identifying Phishing Scams Disguised as DMCA Takedown Notices

March 2022

Beware of a new wave of phishing emails targeting nonprofit organizations and disguised as legitimate Digital Millenium Copyright Act (DMCA) Takedown Notices. These emails accuse the targeted nonprofit organization of violating copyright law to coerce them into downloading malicious content that can disrupt organization IT systems and jeopardize sensitive data and information. This article from the law firm Venable LLP describes some of the distinguishing characteristics of legitimate DMCA Takedown Notices, the ways in which phishing scams attempt to emulate these characteristics, and some of the strategies that nonprofit organizations can use to respond to them.

DMCA Takedown Notices are issued as part of a safe harbor framework created by the federal Copyright Act, which shields nonprofits and other organizations from liability for infringing content posted by users on the organizations' websites, social media accounts, and other digital platforms. This means that an organization will not be liable for user-posted content that infringes another party's copyright, provided the organization complies with certain steps (see prior articles from CAPLAW about the DMCA safe harbor here and here). One of these steps is to respond appropriately when the organization receives a notice from a third party claiming that certain material on the organization's website infringes another's copyright. Failure to respond to a DMCA Takedown Notice correctly may invalidate an organization's DMCA safe harbor protection and expose it to liability for copyright infringement. For this reason, it is crucial to differentiate between legitimate DMCA Takedown Notices and phishing scams and to respond accordingly.

CAAs that receive an email or other written notification about potentially copyright infringing material should familiarize themselves with the attributes of a legitimate DMCA Takedown Notice. Such notices must include the following:

1. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
2. Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works;
3. Identification of the material that is claimed to be infringing or to be the subject of

infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the CAA to locate the material;
4. Information reasonably sufficient to permit the CAA to contact the complaining party, such as an address, telephone number, and, if available, an email address;
5. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
6. A statement that the information in the notification is accurate and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

If your CAA receives an email that does not include all of these elements, it is not a legitimate DMCA Takedown Notice, and it should be deleted, left alone, and/or reported. Unfortunately, phishing emails often include all the required information, making it difficult to distinguish them from legitimate DMCA Takedown Notices. **For requirement #3 above, phishing emails typically include a URL purporting to direct the CAA to the alleged infringing material but instead exposing the CAA to malicious content.**

To safely respond to these emails, Venable suggests the following strategies:

1. Before interacting with the email's content, report the email to your CAA's IT department or consultant for closer inspection. Ideally, your IT department or consultant will have the capability to safely view any links in the email. Note that DMCA Takedown Notices require a timely response, so this inspection should be prioritized.
2. Contact legal counsel to evaluate the legitimacy of the email and request advice on how to respond.
3. Consider forwarding phishing emails to reportphishing@apwg.org (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, financial institutions, and law enforcement agencies) and reporting them to the FTC at reportfraud.ftc.gov.

Bearing these strategies in mind, CAAs should continue to employ effective digital security protocols and practices that protect them from phishing scams and other threats to organization data and digital assets.

This publication is part of the Community Services Block Grant (CSBG) Legal Training and Technical Assistance (T/TA) Center. It was created by Community Action Program Legal Services, Inc. (CAPLAW) in the performance of the U.S. Department of Health and Human Services, Administration for Children and Families, Office of Community Services Cooperative Agreement – Award Number 90ET0482-02. Any opinion, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of HHS and ACF. The contents of this publication are intended to convey general information only and do not constitute legal advice. Any communication through this publication or through CAPLAW's website does not constitute or create an attorney-client relationship. If you need legal advice, please contact CAPLAW or another attorney directly.