ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide additional situational awareness about the growing use of deefake tools in targeted phishing and social engineering attacks against organizations.

Why this matters

With the growing normalization of fully remote working conditions and the hiring of foreign workers that remain working abroad, the opportunities for threat actors to present themselves as other people, either known or unknown to the organization, have greatly increased thanks to the advent of deepfake technology.

Overview

Over the past several years, AI models have been developed to specifically be able to alter multimedia, mainly audio and video, so that highly realistic synthetic media can be produced with ever fewer computing resources. These final results are known as deepfake media.

The technology has been greatly exploited in the realm of cybercrime, mainly for the purposes of financial scams[1]. These scams make use of manipulated videos meant to trick the viewer into believing that a major social figure is indeed giving their support to the scammer's product/service. While these scams are still only targeting individuals, it is possible that in the future we could see such techniques being used against organizations.

Such capabilities have already been exploited against major organizations, be it through voice manipulation[2] or image manipulation. These techniques build on top of the already existing "CEO Fraud" scam by adding further legitimacy to the malicious actor's impersonation of key figures within organizations.

Likewise, the use of Deepfakes complicates the verification of a remote candidate's identity[3], leading to cases where malicious actors, with the help of leaked PII (personal identifiable information)[4], will be able to disguise themselves during video and phone interviews in order to be hired by the target organization.

Recommendations

Recommendation #1: Enforce internal policies and procedures

ORNA **strongly recommends** that organizations strictly adhere to their internal policies and heavily discourage the circumvention of these, particularly for the purposes of authorizing financial transfers and internal system accesses.

Recommendation #2: Implement individual digital signatures

ORNA recommends that organizations implement digital signatures for employees, particularly those working remotely, for the purpose of validating their identity. For workers from countries that issue eSignatures[5] to their citizens, the use of these for the purpose of signing documents should be encouraged.

Recommendation #3: Implement the Zero Trust Security Model

ORNA recommends that organizations implement a security model based on zero trust[6] so that employees have access to only the resources they need in order to perform their tasks, thus limiting the potential damage that a malicious actor can cause.

References

1. https://unit42.paloaltonetworks.com/dynamics-of-deepfake-scams/
2. https://bloomberg.com/news/articles/2024-07-26/ferrari-narrowly-dodges-deepfake-scam-simulating-deal-hungry-ceo?leadSource=uverify%20wall
3. https://blog.knowbe4.com/how-a-north-korean-fake-it-worker-tried-to-infiltrate-us
4. https://krebsonsecurity.com/2024/08/nationalpublicdata-com-hack-exposes-a-nations-data/
5. https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eSignature
6. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.
Sincerely,
ORNA Team