Don’t Fall for Dark Web Sextortion Scam

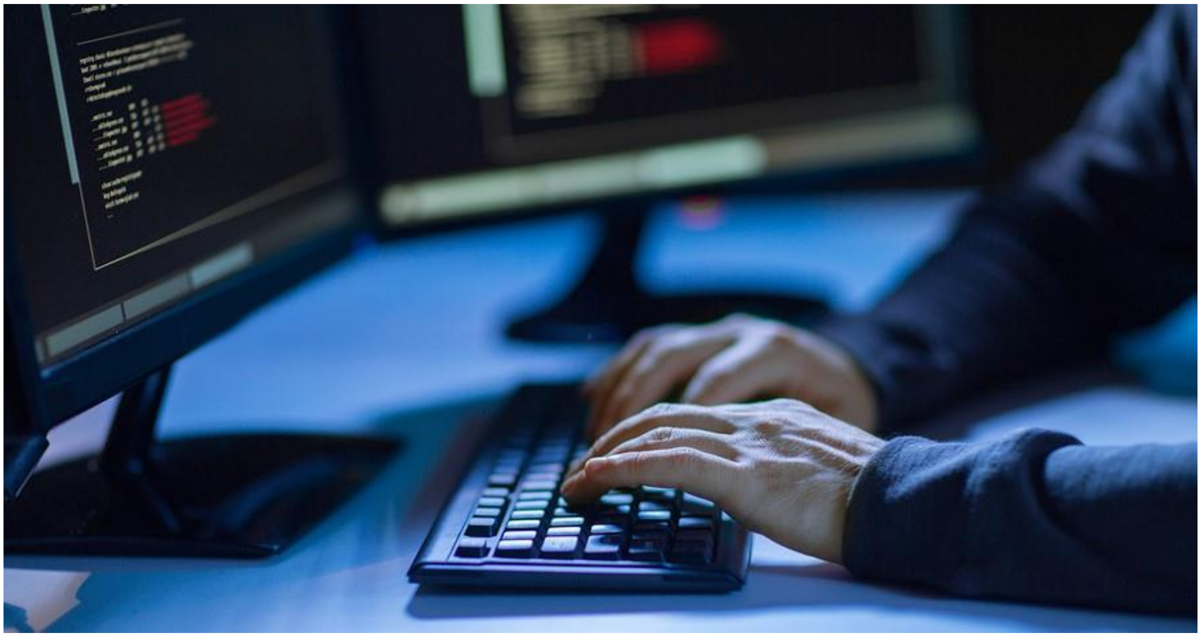
A wave of fraudulent emails containing real user data obtained from the dark web is hitting computers around the world. The emails include a variant of an old online phishing scam termed ‘sextortion’. This dark web sextortion scam leverages digital-age fears to blackmail recipients and targets computer users in large numbers.

> *Dark web sextortion scam criminals fraudulently blackmail victims into paying a ransom to avoid the distribution of an embarrassing video to family, friends and co-workers.*

The message claims to have been sent from a hacker who’s breached your computer and used your webcam to record a video of you visiting a porn website. The criminal threatens to email the video to your contacts unless you pay a substantial ransom, usually in Bitcoin, which is difficult to trace.

This time, the scam employs a new wrinkle to make the fraud more believable. The emails received reference real passwords, likely obtained from the dark web. Passwords stolen in numerous recent large-scale security breaches often find their way to the dark web, where they are sold to scammers.

> *“The dark web sextortion scam has been operating for some time,”* stated Almi Dumi, CISO, eMazzanti Technologies. *“Criminals keep using it because some people motivated by fear pay the ransom. Don’t be one of those people. It’s not a bona fide threat.”*



Oh no! They have my password!

To sound authentic, the dark web sextortion scam email message may begin like this:

> "I'm aware that <*a password previously used on your computer*> is your password."

This is probably a real password that you used sometime in the past. Passwords, such as this are sold in bulk on the dark web to facilitate emails to thousands of victims. The scam works because a small percentage of those who read the email panic and pay the ransom.

Disregard Dark Web Sextortion Scam Emails

eMazzanti urges customers to ignore threatening dark web sextortion scam emails. To explain, a company cyber-security expert describes how criminals send thousands of these fraudulent emails hoping to persuade even just a few of the victims to pay the sextortion ransom based on their false claims. With this in mind, the company recommends these steps as an appropriate response:

How to Handle a Dark Web Sextortion Scam Email

- Ignore and delete the email immediately.
- Don't reply to the email or click any links.
- Do not pay the extortion ransom.
- Inform the FBI if you want to help catch the criminals.
- Reach out to eMazzanti Technologies for dark web ID protection.

Accordingly, the FBI recommends reporting any scams like these to IC3.gov, the FBI's Internet Crime Complaint Center.

Dark Web Identity Protection

Dark web sextortion scam criminals use stolen passwords to make their threats credible. Moreover, these passwords have usually been purchased on the dark web from hackers who obtained them in large scale security breaches. Therefore, if an individual's information has been stolen in a past breach, they may be more likely to be targeted in this type of attack.

eMazzanti Technologies offers professional services related to dark web identity protection. In addition to performing a thorough dark web search and domain monitoring, the company goes a step further and helps with remediation and improving its clients' security posture.

Security Awareness

Security awareness in business is very important. Thus, management must ensure staff is trained to recognize and avoid these threats. Information Security evolves quickly, so should your controls and understanding of it.

> *Security is the responsibility of everyone. Make the information available to ALL your staff and test your security posture on a regular basis.*

To remain vigilant and updated on information security's latest threats, subscribe to the United States - Computer Emergency Readiness Team mailing list at www.us-cert.gov. Or, follow your IT department or IT security service provider's recommendations and keep up with the latest news and alerts.