Verifone SECURITY ADVISORY

Verifone Security Advisory

September 28, 2016

***DISCLAIMER**: This advisory is provided "as is" for informational purposes only. This security advisory may be shared with Verifone clients. Verifone does not provide warranties of any kind regarding any information contained within.*

Verifone continues to receive reports that scammers are contacting Verifone merchant clients posing as Verifone Help Desk agents in order to obtain sensitive payment systems information from unsuspecting merchant employees.

How it works:

Merchants receive a phone call from someone posing as a Verifone Help Desk associate stating that they need access to the merchant's internal systems so that they can perform a mandatory software upgrade. The fraudster asks the merchant to provide sensitive payment processing information that could later be used to perpetrate fraud.

IMPORTANT -- the Verifone Help Desk:

Always provides formal pre-notifications prior to performing any system upgrades or patches
Never requests sensitive payment credentials

You can help protect your organization by following these simple steps:

- Always verify unsolicited callers. If a caller asks you to disclose information, make payments, process transactions or make changes to systems or terminals, be sure to:
  - Ask the caller to identify the company they represent and details of their office number.
  - Use the internet to verify the caller's phone number and other information they provide.
  - Talk to your supervisor, payment provider or terminal manufacturer before you proceed.
- Be suspicious of any "urgent" communication that asks you to confirm or provide payment system, personal or financial information over the Internet or phone.
- Do not open any email attachments if it's not clear what they are related to. It could be a virus.
- Think before you click. Don't click on links within emails if they look suspicious in anyway. Even if the email is from a trusted source – be sure to verify before you proceed. A quick phone call should resolve any suspicions.
- Never share your login credentials or passwords.

Bottom line -- if you have any doubts about the authenticity of any communication, make every effort to validate the credibility of the request before you take action.

Josh Davenport
Security Director, Americas
Verifone
88 W. Plumeria Drive | San Jose, CA 95134 USA
T 408 232 7912 | M 650 863 5314
joshuad4@verifone.com