



New Scam Alert

Tech Phishing Email



Our Elder Financial Safety Center (EFSC) staff helped a client recently who received this phishing email. Luckily, the client called us before calling the listed phone number or replying to the email. We were able to help him identify the email as a scam, prevent him from losing money, and save him from possibly becoming a victim of identity theft.

Why it looked real:

- Tech Panda is a real company
- They used an implied threat to charge the client's credit card a significant amount of money
- They use technical words like "activation," and "installation"

How you can tell this is a scam:

- The "From" email address is a gmail.com account not a Tech Panda corporate email address (@gmail.com instead of @thetechpanda.com)
- The address line does not address you by name. It says "Dear email address"
- There are multiple mistakes in grammar, punctuation, and word choice
- It does not have the company logo
- They are using a non-American date format with the year first
- The payment method is not specific to one credit card company

What to do if you suspect a scam email

If you see any of the above scam warning signs, don't click on anything! If it is **not** a company you do business with, either delete the email or report it in the following two steps:

Step 1

- o If it was an email, forward it to the Anti-Phishing Working Group at ReportPhishing@apwg.org.
- o If it was a text message, forward it to SPAM (7726).

Step 2

- o Report the phishing attack to the FTC at ReportFraud.ftc.gov.

If you are concerned about your bank account or credit card being charged, call your bank or credit card company directly to confirm if the amount was taken. The customer service number will be on the back of your payment card or on your monthly bank statement. If you are still unsure, call us at the EFSC, and we can help.

If it **is** a company you patronize, still don't click on anything in the email! Leave your email and go to the company's official website for their company contact information. Either call or email their legitimate customer service representatives. Usually, the companies are happy to help because they don't want you to fall prey to scams and lose money either. They want their customers to be able to afford to buy their legitimate product.

How can the Senior Source help?

If you need to know more ways to spot scam emails or help with protection or prosecution after being hacked, contact our Elder Financial Safety Center. We offer classes, online training, and personal counseling.

You also can review the documents in the [Frauds and Scams spotlight section](#) of our resource center. Our video, [Protect Yourself from Phishing](#), is particularly helpful.

The Federal Trade Commission [webpages](#) on how to recognize and avoid phishing scams is another useful resource.

Contact Julie Krawcyk at JKrawcyk@TheSeniorSource.org or call (214) 525-6157.

From: Renewal Update Notification

<matteherock6466@gmail.com>

Date: January 18, 2022 at 6:21:42 AM CST

To: texmont@gmail.com

Subject: Thank you for your order- G3VET-7VY/32S7

TECH PANDA INC.

Date:2022-01-18

Dear person@domain.com,

Thank you for choosing the auto renewal plane on TECH PANDA INC., from 2022-01-18.

As you already performed payment, there is nothing else you need to do. However, we recommend you keep this for future reference.

Your order

Reference no.: GhVET-8VY/h2S8

Payment method: VISA/MasterCard

Order date: 2022-01-18

Grand total: \$388.78

Support information

Need technical support? For product installation, activation and other technical support

issues, please contact at

+1 [320] 523_6171,

Thank you,

TECH PANDA INC..

Team.