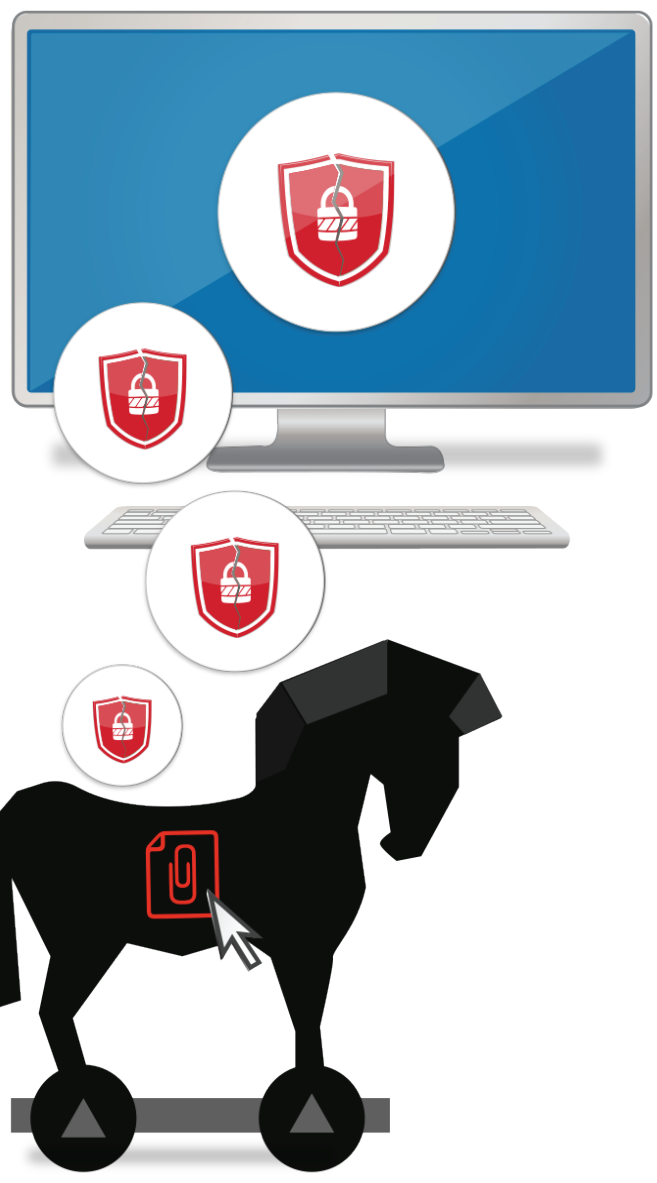
AttackSpotlight

Fraudulent Emails Deliver Trojan

This Thief Takes Everything



Attackers are using fraudulent emails to deliver a malicious program called a trojan. These emails appear to be from reputable sources and have links or attachments to common documents (e.g., an invoice). Clicking the link or opening the attachment installs the trojan, which hides on your device and causes significant harm.

This trojan is particularly dangerous. It can:

Capture **all** credentials on your device, including those saved in browsers

Steal available emails on your device

Install additional malicious software

Spread quickly across your organization's network

What do I look for?

This is one example of an email with a malicious attachment. There are many others, including emails that ask for payment of invoices or correlate to major events or holidays.

1 **From:** Bankofamerica Business <Pradip.Hirase@gtpo.net>
Subject: Account Alert: Bill Pay Alert
To: Savannah Jackson<sjackson@circuitenergy.net>

2 Payment_Remittance_Advice_4463427.pdf
19 KB

Bank of America

Hello,

3 You scheduled a payment of $2,900.54 for your account ending in 2922.

4 For details of a recent payment made to you, please see the attached payment remittance advice. If you have any queries or questions, our contact details are printed on the remittance advice.

Payment_Remittance_Advice_4463427.pdf

5 Bankofamerica. Forward Thinking.
Head of Bus Banking Customer Support

1 Examine the Sender

Would Bank of America use an unusual domain like @gtpo.net? Companies usually have their own domains.

When examining the sender's address, make sure the domain matches what you expect.

2 Consider Attachments

Are you expecting this attachment? Do the file name and type match this email's purpose and subject?

Be wary of odd or unexpected attachments. This one downloads malicious software called a trojan.

3 Consider Content with Context

Do you have an account ending in 2922? Did you schedule a payment for $2,900.54?

Scammers make up details that seem feasible to trick you.

4 Consider Requests

Were you expecting a payment? Is it odd that this information is in an email about another topic?

The payment details are purposely vague to entice you to open the attachment.

5 Notice Small Details

Did you notice the misspelling of Bank of America (Bankofamerica)?

What about the odd abbreviation for business (Bus) in the signature?

Small details like this can indicate a scam.

How do I protect myself?

If you get an email asking you to open an attachment or click a link:

Don't open the attachment or click the link.

Carefully examine the email.

Looks legitimate: Call, message, or send a new email to the sender to verify the email and any attachment. Never reply to the initial email.

Looks suspicious: Report it to the appropriate people in your organization or to your email provider.

proofpoint

Security Awareness Training