Social engineering – the Spiked Punch

2018 Data Breach Digest

verizon

The situation

It began on a Monday morning in February. It was like any other day in the Finance department: a team meeting, weekly task list, and a mountain of emails within my inbox. In that pile, I came across what appeared to be a standard email from a long-time vendor.

This email was like many I'd received and actioned every day. It requested a payment and contained a company invoice with bank information for a wire transfer.

I looked at the banking information and noticed that the account was not in our system. With all due diligence, I replied to the requester requesting information. They explained that the account belonged to a subsidiary of the vendor and they supplied me with a stamped letter of authorization. The sender also requested an email confirmation when the transfer occurred.

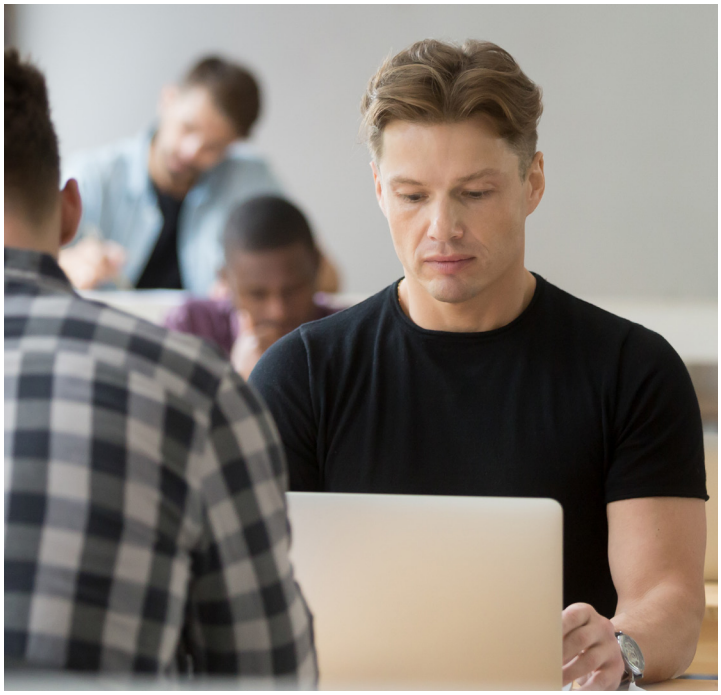
This wasn't unusual as vendors often requested modifications to invoices. With a volume of similar transactions to plow through, I barely gave it a second thought.

On the day of the transfer, I sent a confirmation email to the requester. A short while later they replied indicating that the bank had received the transfer, but due to "in-country terrorism concerns" the money would be returned.

The requester then asked if I could resubmit the payment but split it into four equal payments. Not wanting to be late, I wasted no time in resubmitting the transfers. They thanked me for my customer service and professionalism.

Mitigation tips

- Review sender email addresses and domains; look for misspellings; confirm emails originate from official corporate customer addresses
- When in doubt, pick up the phone and verify customer requests; confirm requesters are approved vendor contacts through a supplier master repository database; confirm money requests through independent channels other than email



Investigative response

The next day the VPs of Finance, IT Security and Legal called me into an urgent meeting. Before I could even take a seat, they asked "why did you transfer money to a non-approved account? What possessed you to resubmit the transfer into four separate transactions?"

I sat up straight and explained the events leading to the transfers. Less than a minute into my explanation, I was cut-off. It was explained that I was involved in a confidence trick and that I had fallen prey to a fraud, potentially costing the company hundreds of thousands of dollars.

The barrage of questions came thick and fast. They wanted to know why I hadn't validated the email address, how I'd missed the email domain being misspelled by one character, why I hadn't validated the request with a co-worker or matched the invoice to the packing slip and purchase order.

The sender had obtained valid account information along with an "official" looking letter from a parent company we do business with. I later discovered that one of our third-party vendors used a personal web email account to conduct business with the Accounts Payable team. That personal account had been hacked.

The fraudster obtained information from previous email correspondence regarding our internal processes and contact information for payment requests. With this information they created an email address mimicking the legitimate third-party vendor's email. It was misspelled by one character.

Phishing email indicators

- Examine the sender email address; look for typos or mismatched email domain names
- Examine the email message; look for misspellings; be cautious of requests for "urgent" or "immediate" action
- Be cautious of embedded hyperlinks; hover your mouse over link to reveal domain name

BALANCE OVERDUE!

Kimberly Jones <kjones@spoofedemailaddress.com>

Sent: Mon 10/17/2018 5:09 PM

To: Smith, John

Cc:

Dear Mr Smith,

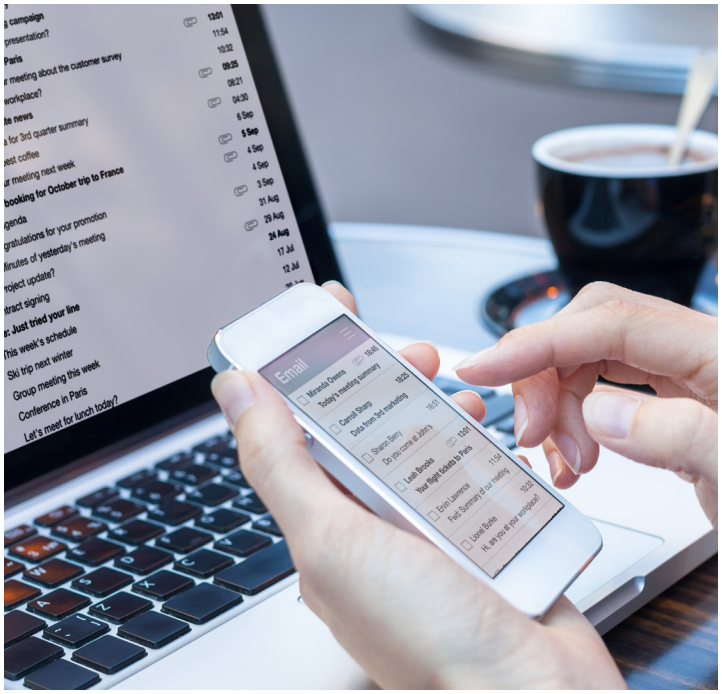
Payment for invoice #4327394 is over 90 days late. Please click here to pay now and avoid being sent to collections.

Regards, Kim Jones

Account Representative

Mitigation tips

- Segregate duties: a junior employee sets up the wire transfer and a senior employee reviews and approves the transfer
- Implement internal controls for matching packing slips and purchase orders to payment invoices
- Implement a vendor management policy requiring vendors use a secure corporate email system; prohibit using personal web mail accounts for business



Lessons learned

When the dust settled, we had an email invoice payment request gone bad, large sums of money transferred to a bank account, and an Accounts Payable employee left wondering what went wrong.

Just like the money, I wished I could just vanish. This incident taught us several valuable lessons which we took action on right away:

Mitigation and prevention

- Review sender email addresses and domains; look for misspellings; confirm emails originate from official corporate customer addresses
- When in doubt, pick up the phone and verify customer requests; confirm requesters are approved vendor contacts through a supplier master repository database; confirm money requests through independent channels other than email
- Segregate duties: a junior employee sets up the wire transfer and a senior employee reviews and approves the transfer
- Implement internal controls for matching packing slips and purchase orders to payment invoices
- Implement a vendor management policy requiring vendors use a secure corporate email system; prohibit using personal web mail accounts for business