FRAUD AWARENESS: SOCIAL ENGINEERING

Cambridge Global Payments

Cambridge Global Payments is a major participant when utilizing the financial system to effect and promote the business interests of our customers. As such, we understand and take our role in ensuring that we and our customers can confidently operate efficiently and securely seriously.

It is possible to detect and prevent fraud. Regardless of how secure your business is, it is often the human element that falls prey to social engineering methods. While you cannot discount the human element, you can learn to anticipate how employees and colleagues might fall victim to social engineering tactics and develop measures to mitigate the risk.

Nefarious characters will go to great lengths to educate themselves on the inner workings of your business, your activities, your processes, and employees.

Wire and Email Fraud are highly successful and lucrative for fraudsters and are relatively easy to pull off with a little research and clever tactics. The first step in risk mitigation is to understand the most common types of social engineering scams that have befallen many businesses.

Some common social engineering tactics are **Caller ID and Email Spoofing**. It is relatively simple to make an email or caller ID *appear* to be legitimate or seemingly match one that you/your employees are used to seeing on a regular basis.

That email from your vendor asking you to update the bank account information appears completely legitimate - - doesn't it? Or that email from your company President asking you to send funds to him while travelling?

If it was fraudulent, your firewalls and security features would catch it - - - - right? You could be very Wrong!

Unfortunately for several businesses by the time a scam has been detected, it is far too late.

Pretexting. Criminals create a false 'pretext' for contacting one of your employees. They may pretend they are a prospective supplier, research firm, bank or government agency asking for the names of employees, banking information, login credentials or something seeming equally as innocuous. Any information they gain can thereafter be used to build a profile which in turn allows the fraudster to pose as an employee and ultimately gain access to your business, personal or financial information, your systems or customers. They may move on to scam your business using **Caller ID or Email Spoofing**.

Phishing *[pronounced Fishing]* is a very common online scam. An email is sent with the intent to manipulate the recipient into disclosing personal, business or financial information. Typically, these phishing scams attempt to play on emotions or sympathies. They will stress an urgency and will contain a link often accompanied by a deadline date for you to access and input your information. By disclosing any of these details you are essentially putting the fraudster a step closer to accessing your accounts. Fraud can have far reaching and devastating impact to your life or business. **A legitimate urgent situation would never require anyone to send personal, business or financial information by accessing a link.**

Characteristics and Behaviors to always be aware of:

- Text contains incorrect spelling, phrasing or grammar or uses wording that is uncharacteristic
- Customer is difficult to contact and prefers email communication
- Email address differs very slightly from that which you are used to
- Email domain is different from that which you have historically used or is from a free service provider such as Hotmail or Gmail when it should contain a business domain
- Transaction may be inconsistent with historical transactions
- Contact applies significant pressure for the deal to be processed prior to receiving full verification
- Unexplained sense of urgency and a willingness to accept shortcuts
- Unexpected changes to payment or beneficiary details

How do you protect your business? We recommend taking steps similar to what Cambridge does. Awareness and Training are key. Employ tactics that are designed to verify and validate the information your employee is receiving, before making any changes to payment details.

If you receive an email request to alter banking information, **phone your contact at your vendor's company to verify that banking information has been changed.**

If you receive a phone call requesting a change to banking information, take the time to place a phone call to the number you have always used for your contact – **not the phone number that just appeared on caller ID when the request to change banking information was received** – and verify that banking or payment details have changed. You may just learn that your or your vendor's email or phone network have been compromised, and by taking the few minutes to verify the information you have just saved you and your vendor from being scammed.

cambridgefx.com
info@cambridgefx.com