e2r Alert!

Scams Targeting Employees

Over the last few months there has been an increase in phishing emails/texts/calls targeting everyone, including employees while at work. While employers can take proactive IT steps to limit these attacks, some will get through – especially if they target the employee's personal phone or email. We have some suggestions to help protect you and your teams from a scam.

Here are some examples of the common scams we are hearing about:

Scam 1: Urgent Help Required

- A scammer sends an employee an email that appears to come from a senior executive in the company.
- The email claims that the executive requires urgent support to buy gift cards for employee rewards or requests a large money transfer.

Scam 2: Head Office Support Required

- A scammer calls an employee and claims be from "head office", the call display verifies this information.
- They share that there are problems with one of the financial products (ex. gift cards) and that they need their assistance to "verify" credentials.
- The employee is then asked to select some prepaid cards, activate them, and provide the information to the scammer.

Scam 3: Payroll Change

- A scammer sends an email to a member of your payroll team, the email appears to come from an existing employee.
- The scammer requests that their direct deposit information is updated and provides new banking credentials.

Upon hearing of these scams, we have no doubt that you as the reader would believe that this could never work, your staff are too tech savvy to fall for such obvious scams. Unfortunately, these do happen and scammers are successful in getting employees to send/verify/change information per the scammers request.

These scams appear to gain traction because the request appears to come from a credible source. The scammer is skilled at playing on the employees' vulnerabilities and has them act quickly for an urgent/confidential business need. The scammers are so convincing that the employee does not stop to question why they are being asked to provide money or financial information in an unusual way, or to verify personal/financial information.

What can you as an employer do?

Training your employees is key to ensure they remain vigilant and that they question any odd/non-standard or "rush/urgent" requests that come in. Internal processes could include:

- Ensure employees check the sender's information before taking action on anything. Questions they should ask: Does the email address match the senders name and what is on file? Is the phone number actually a registered number for head office? Have I tried calling the person back on a known company phone number?
- Implement a company practice for employees to call their immediate manager prior to acting on any financial requests, regardless of urgency – on the manager's existing company contact number – if the scammer claims they are the manager and they have 'lost' their phone – that is a serious red flag.
- Develop and carefully communicate a company "CODE" word. This could be used as one way to verify that the request is coming from a reputable source – change codes monthly.
- Verify that the companies email filters/blockers are up-to-date to ensure most of the scams are blocked prior to hitting employees' inboxes.

Open communication with your employees helps ensure that they act cautiously and follow company protocols should any odd/unusual requests come in.

In the unfortunate event that you are the victim of a successful scam, you will want to report it to the police immediately and conduct an internal investigation. Determining areas of improvement in your Companies process should be a key focus to prevent future attacks. Depending on the findings of the investigation and the responses from those involved, formal disciplinary action may be warranted.

If you have any questions about employee scams or what you can do following a successful scam, please do not hesitate to contact ClientCare.