CASE STUDY

DIAMOND IT
your potential. our passion.

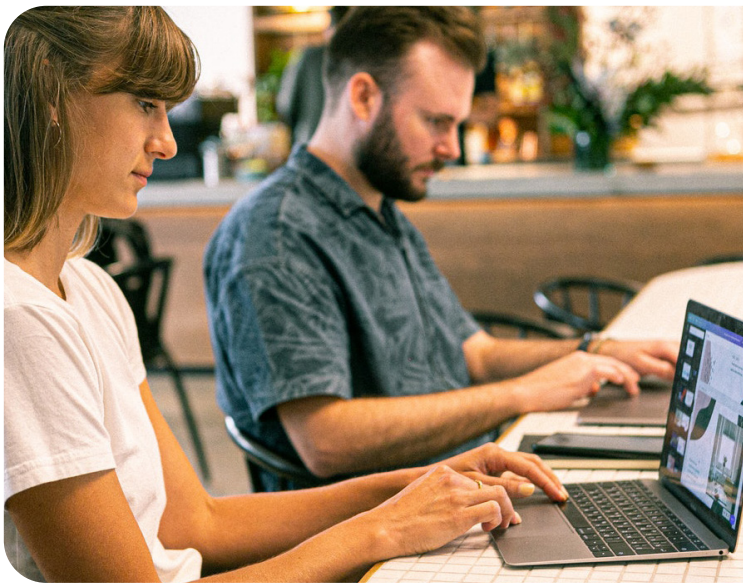
Cybersecurity Experts Prevent Corporate Bank Account From Being Wiped Out

One clever email nearly cost one of our clients an emptied bank account. The targeted client is a small but global business in the oil and gas industry with headquarters in Kern County. The organization, founded in 1986, has entrusted DiamondIT with their IT environment and cybersecurity since 2009. But as they quickly learned, even with the most sophisticated and complete cybersecurity management available, any company is vulnerable to a phishing email sent from a Gmail account.

THE DEADLY COST OF ONE TARGETED EMAIL

The company was targeted by a phishing email, sent to an employee in the finance department, asking for sensitive banking information. The spoofed email ended up in the inbox, bypassing initial spam filtering because it originated from Gmail. The recipient didn't suspect the email was nefarious, because it appeared to be "from" their boss, even using the correct name.

Once the employee received the email, they responded that they would provide the requested account information in the morning, as it was past working hours. Without intervention, the employee would have done exactly that. All of the money in that account would have been wiped out.



AN INVESTED CYBERSECURITY TEAM INTERVENES

The company narrowly escaped a potentially devastating loss of funds. Though the company targeted works in a niche industry, they are not particularly well-known. This criminal took the time to thoroughly research the organization and craft a convincing email.

With the employee's reply, DiamondIT's email security service immediately flagged the communication as a potential threat to the company and placed a block on further communications with the suspected hacker. The system subsequently notified our expert security team who sprang into action. DiamondIT notified the company's general manager, explaining that the email would not have looked suspicious. The chief concern was ensuring that no financial transactions took place and that the company recognized the email threat.

CYBERSECURITY SERVICES IS JUST THE BEGINNING

Hackers don't just go after the big names. They go after companies where they are most likely to be successful. If they can find the right names and company responsibilities online, they can use that to launch a successful attack against you.

Under the direction of DiamondIT's Chief Information Security Officer Cody Cooper, a Certified Information Systems Security Professional, DiamondIT follows the NIST Cybersecurity best practices framework to offer multi-layered protection, threat detection, identification of impact, response and recovery from attacks.

DiamondIT continues to work with the client to help them create a company culture of cybersecurity. This means appointing a security officer within the company, managing policies impacting security policies and providing cybersecurity awareness training that employees successfully complete.

KNOW WHAT YOUR IT PROVIDER IS DOING TO ENSURE YOUR PROTECTION

If your IT provider cannot talk to you about their security precautions, you should assume you are not secure. When you work with DiamondIT, you get a relationship with a team of experts who are your IT guard dogs. If something is wrong, chances are we're calling you before you're calling us. We believe that's the way it should be.

Don't trust your cybersecurity or IT support to anyone else.

Contact us today:
www.diamondit.pro/contact/ or (877) 716-8324.

WHY YOU NEED A SECURITY OFFICER

An internal security officer would ensure:

- All employees are successfully completing cybersecurity training (even executives)
- When needed, remedial cybersecurity training is conducted
- Training is frequent and varied enough to provide adequate protection
- Company information is classified according to value
- Policies are enacted to ensure better protection of company information