



## A Construction Company Gets Hammered by A Keylogger

### SCENARIO:

A small family-owned construction company made extensive use of online banking and automated clearing house (ACH) transfers. Employees logged in with both a company and user-specific ID and password. Two challenge questions had to be answered for transactions over \$1,000.

The owner was notified that an ACH transfer of \$10,000 was initiated by an unknown source. They contacted the bank and identified that in just one week cyber criminals had made six transfers from the company bank accounts, totaling \$550,000. How? One of their employees had opened an email from what they thought was a materials supplier but was instead a malicious email laced with malware from an imposter account.

### ATTACK:

Cyber criminals were able to install malware onto the company's computers, using a keylogger to capture the banking credentials.

*A keylogger is software that silently monitors computer keystrokes and sends the information to a cyber criminal. They can then access banking and other financial services online, using valid account numbers and passwords.*

### RESPONSE:

The bank was able to retrieve only \$200,000 of the stolen money in the first weeks, leaving a loss of \$350,000. The bank even drew over \$220,000 on the business' line of credit to cover the fraudulent transfers. Not having a cybersecurity plan in place delayed the company response to the fraud.

The company also sought a cybersecurity forensics firm to:

- help them complete a full cybersecurity review of their systems
- identify what the source of the incident was
- recommend upgrades to their security software

### IMPACT:

The company shut down their bank account and pursued legal action to recover its losses. The business recovered the remaining \$350,000 with interest. No money for time and legal fees was recovered.

### LESSONS LEARNED:

- ① Get notified – set up transaction alerts on all credit, debit cards and bank accounts.
- ② Restrict access to sensitive accounts to only those employees who need access; change passwords often.
- ③ Companies should evaluate their risk and evaluate cyber liability insurance options.
- ④ Choose banks that offer multiple layers of authentication to access accounts and transactions.
- ⑤ Create, maintain, and practice a cyber incident response plan that is rapidly implementable.
- ⑥ Cyber criminals deliver and install malicious software via email. Train employees on email security.

### DISCUSS:

- Knowing how the firm responded, what would you have done differently?
- What are some steps you think the firm could have taken to prevent this incident?
- Is your business susceptible? How are you going to reduce your risk?

### RESOURCES:

- NIST Small Business Cybersecurity Corner: <https://www.nist.gov/itl/smallbusinesscyber>
- National Cybersecurity Alliance: <https://staysafeonline.org/cybersecure-business/>