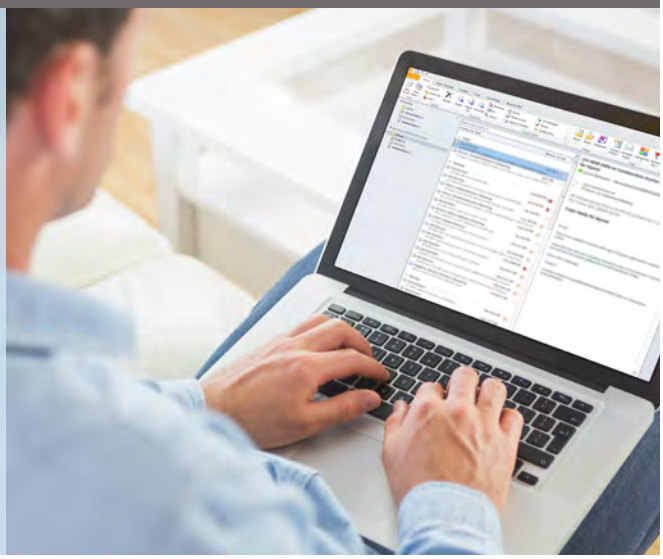
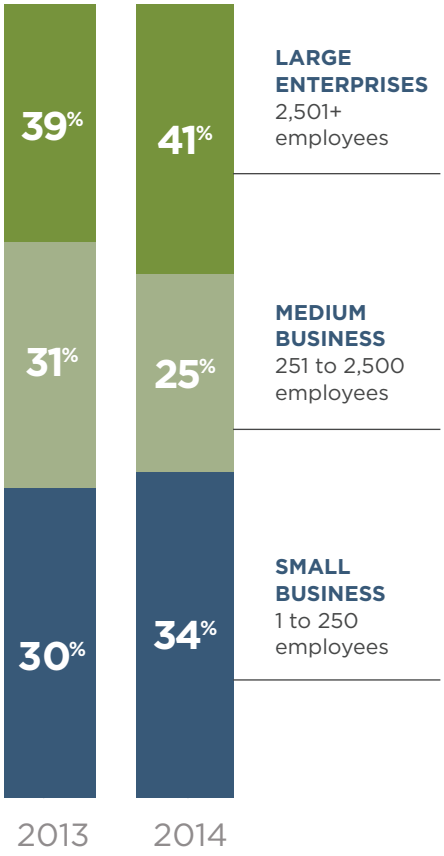
CRIME INSURANCE – DECEPTION FRAUD COVERAGE

Critical coverage to help your business prevail against crimes of deception and trickery.



Spear Phishing Attacks by Business Size[1]



DECEPTION FRAUD COMES IN DIFFERENT FORMS

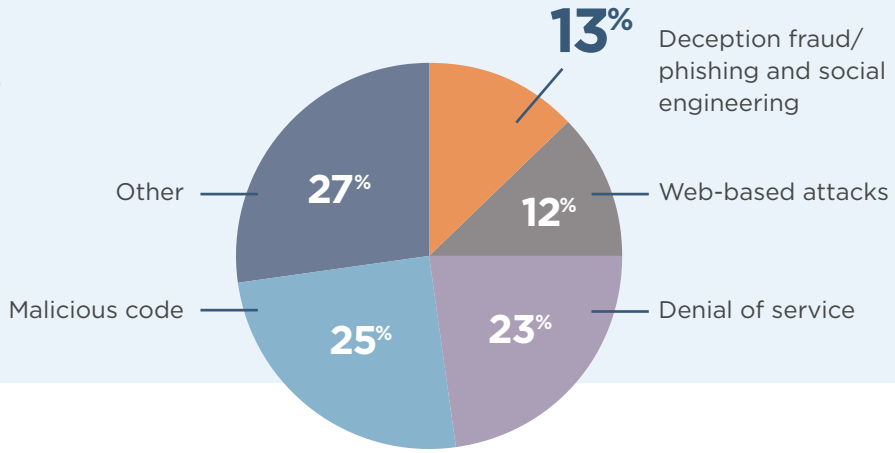
It's happening every day, even at the best-managed companies. Unsuspecting employees are intentionally misled into sending money or diverting payments to imposters. They're misled by fraudulent information they receive in an email, text, instant message, telephone or other electronic means that appears to be from a legitimate vendor, client or even fellow employee. At The Hartford, this type of trickery is called deception fraud. With The Hartford's deception fraud endorsement, you can help protect your business from a wide variety of scams.

ABOUT DECEPTION FRAUD

- Commonly referred to as social engineering, these criminals use various types of confidence tricks such as phishing or spear phishing, pretexting, impersonation or IVR/phone phishing.
- Companies of all sizes are targeted.
- There are over 100,000 deception fraud attacks each day.[2] Attacks on businesses have risen 91% over the prior year.[1]
- Highly sophisticated, surprisingly successful and difficult to detect. They play on the desire of most people to trust, and company policy to be helpful.
- There's little known technology available to completely counter it.
- A lack of security protocols used by business partners, vendors and customers can lead to a deception fraud scheme.
- Key employees with access privileges, banking information, computer system details or wire transfer authority are at most risk of being targeted.[3]

Most costly types of attacks

13% of attacks are tied to tricks (deception fraud), not hacking.[3]



OUR DECEPTION FRAUD ENDORSEMENT

- Is included in all of our Crimeshield® Advanced and Private Choice Ovation® crime insurance policies.
- Automatically added to new and renewal policies; a $15,000 limit with a $5,000 deductible; at no additional charge.
- Higher limits are available; check with your insurance broker or agent.

IMPORTANT WAYS TO HELP PREVENT AN ATTACK

This form of criminal activity has become a huge growth opportunity for fraudsters hiding in cyber-space. Unlike computer hacking, there is little in the way of anti-deception technology a company can purchase to protect against these types of deception and phishing-related events.

Establish Strong Internal Controls

Examples include:

- Provide anti-fraud training inclusive of how to detect deception fraud schemes.
- Authenticate all requested changes to vendor or customer internal bank information.
- Validate requests from vendors and clients with a "call back" procedure to an individual authorized to make such requests and to a previously established number.
- Require next level supervisor sign off on any changes to vendor and client information.
- Require next level supervisor sign off on all wire transfers.
- Validate all internal employee requests to transfer funds.
- Limit wire-transfer authority to specific employees.
- Consider conducting third-party penetration testing.
- Guard against unauthorized physical access.
- Monitor use of social media outlets.
- Develop incident reporting and tracking programs that document incidents or attempts of deception fraud.

Follow Safety Tips Like These

- Stay current with the latest types of deception fraud that are prevalent.
- Educate employees on how to recognize an attack. The best defense is employee awareness through education and training.
- Never release confidential, sensitive or proprietary information to someone you don't know.
- Never forward, respond to, or access attachments within unsolicited emails. Always be suspicious of such emails.
- Identify which employees have access to bank account information, or have authority to make payments or transfer funds. They could be a primary target.
- Hold employees accountable.
- Use cyber security software, and keep it up to date.
- Use mobile device security procedures.
- Use secure Wi-Fi networks.
- Be prepared to respond to an attack.
- Purchase The Hartford's crime insurance with the deception fraud endorsement, available through Crimeshield Advanced and Private Choice Ovation.

CLAIMS SCENARIOS – LEARN HOW OTHER BUSINESSES WERE TRICKED SO YOU CAN AVOID BEING SCAMMED

The following claims scenarios demonstrate some of the ways fraudsters have tricked businesses into sending them money. Now, more than ever, is the right time to have deception fraud coverage from The Hartford.

CLAIM 1	
Deception fraud	Company A received an email, purportedly from the contact person at its China supplier. The email stated there was a problem with the supplier's bank account, and instructed Company A to make the payment to a different bank account in the UK.
Action taken	In response to those instructions, Company A wire-transferred four payments – totaling $250,000 – to the UK bank account.
Result	Company A later learned that: • An imposter (not its China supplier) had sent the email. • The funds it forwarded to the UK bank account had been removed and could not be recovered. **Company A's loss due to deception fraud: $250,000.**

CLAIM 2	
Deception fraud	Company B's vice president received an email that appeared to have been forwarded by the company's treasurer. The email: • Instructed the VP to wire-transfer $1.2 million to the bank account listed in the email. • Provided instructions on where to code the payment. • Included an attachment, which appeared to be an email written by Company B's CEO, containing payment instructions and requesting confirmation when the transfer had been completed.
Action taken	The vice president requested additional backup documentation and was advised that he could use the CEO's email as authorization for the transfer. The vice president then made a verbal request to his assistant to make the wire transfer.
Result	At a later point, the vice president asked the treasurer for the backup documentation, but the treasurer had no recollection of the earlier request. Soon after, it became apparent that the vice president and treasurer had been victims of deception fraud. **Company B's loss due to deception fraud: $1.2 million.**

CLAIM 3	
Deception fraud	Company C did business with an overseas vendor and received legitimate invoices. Company C received an email, purportedly from the overseas vendor, containing: • Instructions to send payments to a new bank account, which was set up in the name of a different company related to the vendor. • An explanation that the bank account had to be changed for tax purposes. • Information about the new bank.
Action taken	Company C made three wire-transfer payments to the new account, according to the email instructions.
Result	It wasn't until the real vendor contacted them for payment that Company C realized it had been the victim of deception fraud. **Company C's loss due to deception fraud: $475,000.**

LEARN MORE. Contact your agent from The Hartford today, or visit us at **THEHARTFORD.COM/CRIME**.

THE HARTFORD

Business Insurance
Employee Benefits
Auto
Home

[1] Symantec Internet Security Threat Report, April 2015, Volume 20

[2] Hillard Heintze The Front Line Report

[3] Ponemon Institute; 2014 Cost of Cyber Crime Study; United States

The scenarios summarized herein are offered only as examples. Coverage depends on the actual facts of each case and the terms, conditions, and exclusions of the issued policy. Please refer to the issued policy to determine all terms, conditions and exclusions of coverage. Coverage is provided by the property and casualty companies of Hartford Financial Services Group, Inc. and may not be available to all businesses in all states.

The Hartford® is The Hartford Financial Services Group, Inc. and its subsidiaries, including Hartford Fire Insurance Company. Its headquarters is in Hartford, CT.

15-0304 © August 2015 The Hartford Financial Services Group, Inc. All rights reserved.