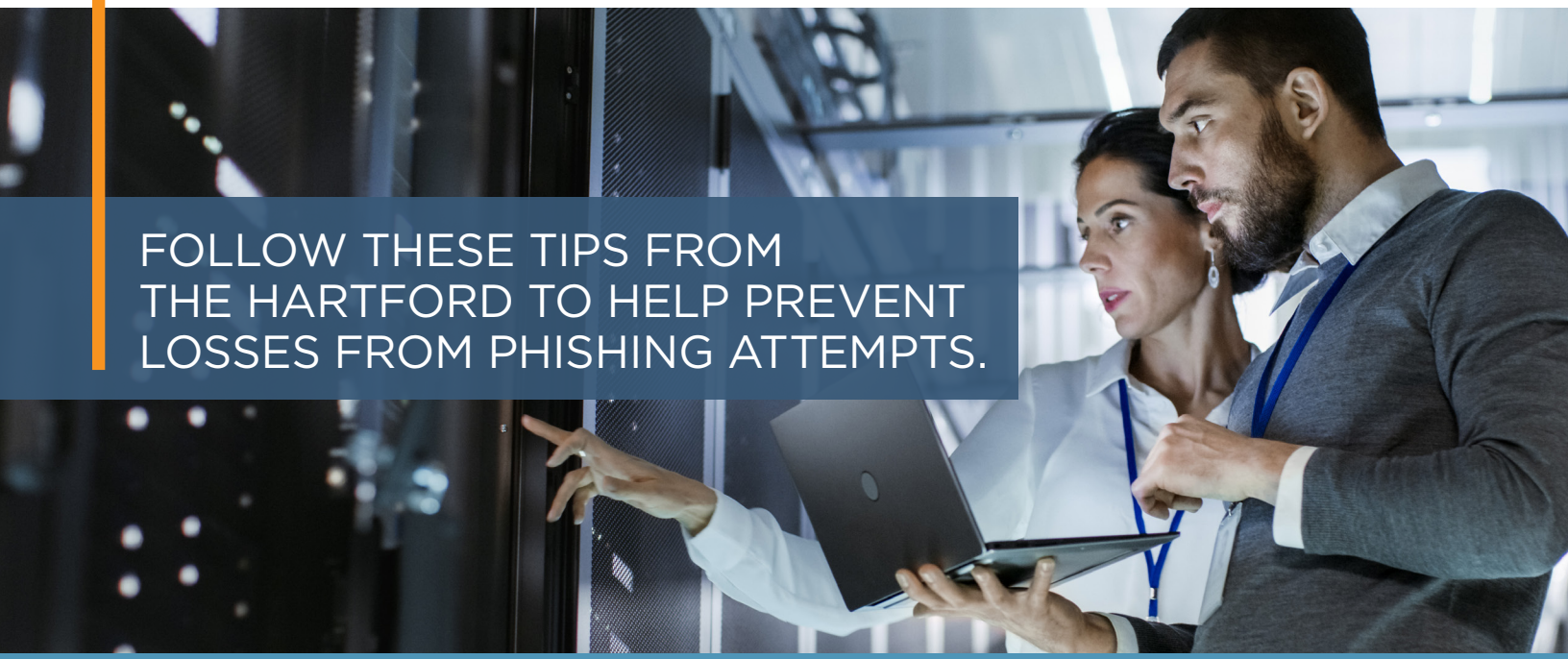

FOLLOW THESE TIPS FROM THE HARTFORD TO HELP PREVENT LOSSES FROM PHISHING ATTEMPTS.

BEWARE OF FRAUDULENT INFORMATION:

Sent through the mail

Sent in emails, texts or instant messages

Conveyed in phone calls intended to deceive or wrongfully extract information/payment

Help protect your business against these crimes with The Hartford's Crimeshield® Advanced and Private Choice Premier®.

It's happening every day, even at the best-managed companies: unsuspecting employees are intentionally misled into sending money, W-2 data or other confidential information to imposters.

They're misled by fraudulent information they receive in an email, text, instant message, telephone or other means that appears to be from someone they know, like a legitimate vendor, client and especially from a fellow employee.

At The Hartford, this type of trickery is called deception fraud.

THE BEST AND FIRST DEFENSE: EMPLOYEE AWARENESS

The weakest link in the security chain is the employee who accepts a scenario at face value and doesn't check its legitimacy.

Employee awareness through education and training is critical. Some tips include:

- **Provide regular anti-fraud training** that includes educating employees on how to recognize and prevent a deception fraud scheme or attack. Hold employees accountable.
- **Stay informed** on the latest spear phishing/deception fraud scams being perpetrated against businesses, and keep your employees informed of the same.
- **Train employees** on what's considered to be confidential, sensitive or proprietary information that should never be released to someone they don't know or who doesn't have a valid and approved reason for needing it.

THE HARTFORD

BUILD DEFENSE MEASURES INTO YOUR PROCESS

Some examples of "best practices" to help you build defense measures against deception fraud include:

Validate information requests.

- Validate all requested changes to vendor or customer contact information and internal bank information.
  - » For example, validate requests from vendors and clients with a "call back" procedure to a previously established telephone number or email address of a person you know to be authorized to make such a request on such vendor or client's behalf.
  - » Require next-level supervisor sign-off on any changes to your vendor and client information.
- *Never* validate a request by utilizing the "reply" function or by calling a telephone number that was provided as a part of the request. Email addresses and telephone numbers should come from the company directory.

Establish a formal process with wire transfers.

- Follow a formal process for validating all employee-to-employee requests to wire transfer funds.
- Limit wire-transfer authority to specific employees.
- Require next-level supervisor to sign off on all "internally" requested wire transfers.

Use your instincts and proceed with caution.

- Be suspicious when someone refuses to provide contact information.
- Never let the urgency of the message influence your careful review and assessment. If the message conveys a sense of urgency, or uses intimidation or high-pressure sales tactics, slow down!

Limit access to sensitive information.

- Guard against unauthorized physical access (theft of keys, access cards, ID badges) to prevent schemes perpetrated through direct access. Keep physical documents locked and secured. Shred documents no longer in use.
- Identify which employees have access to bank account information, or have authority to make payments or transfer funds. Many times, they're a primary target and therefore should be regularly coached on the proper procedure.

Be wary of unsolicited emails.

- Never forward, respond to, or access attachments or links within unsolicited emails. Always be suspicious of such emails.

Keep track of deception fraud events.

- Develop reporting and tracking programs that document incidences of deception fraud or attempts of deception fraud.

SEEK TECHNOLOGY AND COVERAGE THAT LIMIT YOUR EXPOSURE

Here are some ways technology and insurance can help:

- Use cybersecurity software and keep it up to date.
- Use mobile device security procedures and secure Wi-Fi networks.
- Use two-factor authentication to make it difficult for hackers to enter your organization's computer platform(s).
- Randomly test employees with company-created fictitious emails and/or phony phone calls.
- Monitor how successful your protection is by conducting third-party penetration testing.

LEARN MORE.

Contact your agent from The Hartford today. Or visit us at **TheHartford.com/crime**

THE HARTFORD

Business Insurance
Employee Benefits
Auto
Home