

E-mail Risk - Spear Phishing

Incident Details:

Several employees (maybe all) received an e-mail that appeared to be from one of the executive managers asking employees to click on the link in the e-mail to ensure that the organization's new Pandemic Flu plan had all employees' updated contact information and system login information in case employees are forced to work from home.

Why Did This Happen?

Lack of Awareness, General Training and Megaphone Management methods did not engage employees or give them the necessary tools to understand phishing and pharming risks. Employees did not understand incident reporting procedures for phishing risks and were unable to make management aware of the incident.

How Would Better Knowledge Sharing Help?

Management personnel needs to implement customized awareness training and ensure that all employees are engaged and understand their individual roles and responsibilities for preventing risks and responding appropriately.

Who Needs Customized Knowledge?

- Employees
 - IT or IS Department (block web site access, block e-mails)
 - Records Management Person
 - Full-time Employees (branches, other satellite offices, etc.)
 - Temporary Employees
 - Media Spokesperson
 - Risk Department Person
 - Legal Department Person
 - Compliance Department Person
 - Board of Directors
- Third-Parties
 - FBI (threat could be from another state or another country)
 - State Bank Association (any other reports)
 - Vendors (e-mail, Internet, spam, online hosting, etc.)

OK, Then What? (Prevention, Responses, Recoveries and Re-Training)

- Who (if anyone) clicked on the link?
- Who (if anyone) provided information to the link?
- Spyware scans (in case PCs were infected by the link)
- Virus scans
- User Password Changes
- Server Password Changes
- Intrusion Detection Reports
- Internal System Scans
- Suspicious Activity Report
- Customer Privacy Breach – Unauthorized Access Notifications
- Identity Theft Red Flag Procedures (required by November 2008)
- Update Incident Reporting Procedures (lessons learned for next incident)
- Update Incident Calling List



Real-World Example:

Saleforce.com
<http://www.internetnews.com/security/article.php/3709836>

"Most organizational leaders agree that all management is risk management. Unfortunately the biggest and most expensive risks threatening organizations today are Human Factors, and even worse very few organizations have implemented Knowledge management tools, which is exactly why so many embarrassing and expensive management failures are occurring across so many organizations."

- Rick Shaw, CEO Awareity

Next-Generation Knowledge Management Quadrant

