Social engineering attacks, also known as executive impersonation fraud, are among the most difficult workplace crimes to prevent. Perpetrators typically gain an employee's confidence and use that to trick them into transferring funds under false pretenses. Along with insurance, education and awareness are the best defenses against this growing crime.

OUTWITTING THE OFFENDERS:
BHSI'S SOCIAL ENGINEERING PREVENTION PROGRAM

Berkshire Hathaway Specialty Insurance (BHSI) provides qualifying U.S. based private/nonprofit customers with exclusive, complimentary access to the BHSI Social Engineering Prevention Program (SEPP). Provided in partnership with SecurIT360, a leading security firm, SEPP provides those customers with a suite of services and resources designed to help them prevent social engineering fraud and act swiftly to mitigate any suspected incidents.

Real-time Resources, Insights & Training

SEPP supports those qualifying U.S. based private/nonprofit customers with a three-pronged approach that includes a 24-hour hotline, educational and scenario simulation services, and an online portal with information, tips and training materials.

Those qualifying U.S. based private/nonprofit customers and their employees have access to a round-the-clock hotline they can call for confidential coaching and risk analysis if a social engineering event is suspected. The coach will help the caller identify potential red flags — whether in an email exchange or telephone instructions — and take action to avoid an incident or help mitigate ultimate damages.

> BHSI provides SEPP in partnership with SecurIT360, a full-service security consulting firm focused on the physics of securing IT.

24h **24-Hour Access to Experts**

> By training our customers and employees to use the hotline or portal when they suspect social engineering fraud, our Social Engineering Prevention Program helps our customers avoid human error and loss.

Social Engineering, Phishing & Spoofing Simulations and Training

SecurIT360 will work confidentially with those BHSI qualifying U.S. based private/nonprofit customers to execute a social engineering simulation and assess employee response and readiness. This assessment enables companies to evaluate their need for employee education and prevention training and customize programs to their needs.

What is a Social Engineering Event?

Social engineering can take on many different forms and is becoming increasingly difficult to detect. Most attacks target employees with access to company finances and trick them into wiring funds to bank accounts thought to belong to trusted partners, when in reality, the funds end up in accounts controlled by criminals.

Some real-world examples:

A phishing email was directed to a finance executive at a major US-based manufacturer with authority to approve large cash transfers. The email appeared to be written by the company CEO. The unsuspecting executive – per the hacker's well-researched plan – transferred more than $3 million in company funds to a bank in China in an unauthorized transaction.[1]

A fraudulent email sent to the finance department of a US-based money transfer organization resulted in the movement of $30.8 million in corporate cash to fraudulent overseas accounts. Due to the incident, the CFO resigned and the company's stock dropped 14 percent, or approximately $31 million.[2]

[1] 5 Real-World Example of Business Email Comprehensive (resoruces.infosecinstitute.com) [2] IBID

Online Portal - Forms, Training and Education

Those BHSI qualifying U.S. based private/nonprofit customers have complimentary access to SEPP's online portal that includes comprehensive information and education materials to help prevent and prepare to respond effectively to social engineering events. The portal includes:

- Employee training materials and webinars
- Practical tips to 'harden' their organization against attacks
- Real-world examples of social engineering
- Incidents and techniques used by perpetrators
- Information on how to respond to an event, including forms for FBI reporting
- Contact information for a dedicated prevention and response coach.

BHSI Fidelity and Crime Insurance

BHSI writes primary and excess fidelity and crime insurance for a wide range of business segments, including private/nonprofit customers. E&P Package policies are also available for Middle Market risks. *Coverage can be enhanced to respond to Executive Impersonation/Social Engineering losses.*

Our fidelity and crime Insurance is underwritten on the paper of BHSI's National Indemnity group of companies, which hold financial strength ratings of A++ from A.M. Best and AA+ from Standard & Poor's.

For those BHSI qualifying U.S. based private/nonprofit customers, activating your Social Engineering Protection Program is easy.

To register visit https://bhsi.securit360.com

For assistance, email BHSIphishing@securit360.com

Berkshire Hathaway Specialty Insurance