Guidepost

PUTTING A DANGEROUS HORSE OUT TO PASTURE

One of antiquity's most enduring legends is that of the Trojan Horse. The Greeks were unable to breach the walls of Troy after ten years of warfare and had apparently left the outskirts of the city. Instead of their implacable enemy, the Trojans found outside their wall a giant wooden horse which they understood to be a tribute to their stout defenses left behind by the gods or the Greeks. The horse, as we all know, was actually filled with Greek warriors who opened the gates at night after the horse was drawn into the city. The Greek fleet returned and Troy was destroyed.

Among the numerous lessons this scenario teaches is that people can be their own worst enemy. The Trojans believed what they wanted to believe; self-deception proved their undoing. Some 30 centuries later, this lesson remains unlearned and underlies many data breaches and intrusions.

In March of this year, a Federal Reserve Bank transferred about $80 million from the national bank of one country to casinos in two other countries. The ruse was possible because the thieves had compromised the computer network of the victimized national bank and used its credentials to order the transfer. The processor who approved the request completely overlooked two obvious red flags: the money was being sent to private entities and the English spelling was poor.

During tax season, email spoofs designed to steal W-2 forms abound. Typically, someone in a payroll department receives an email purportedly from the CEO or other very high-ranking executive requesting a copy of all the W-2 produced for the last calendar year. The unwitting employee complies and the most sensitive of all personal financial documents get sent to parts and parties unknown. The false email did have the executives name correct, but with a domain name that closely resembled the company's.

Investment firms can fall prey even if they use an independent fiduciary agent which is in place to prevent self-dealing and protect investors. Just like a well-intentioned but misguided employee, such agents have been known to transfer money based upon a spoofed email purporting to be from a principal of the investment firm, but which had a slight misspelling in the domain name.

Each of these incidents succeeded precisely because the attacker decided not to assault the technical walls defending its intended victim, and chose instead to simply trick the humans hiding behind them. People remain the soft

underbelly of any cybersecurity plan. Fortunately, there is an easily installed correction.

Consider two-factor authentication. Requests for documents containing personally identifying information should not be honored by simply attaching the documents to a replying email. Requiring that the document be sent by attaching it to a new email with the address of the requester freshly typed in will defeat almost all such scams. The act of typing will alert the intended victim to the erroneous domain name. Transfers of capital should similarly be confirmed either by a newly typed email or by telephone. Are such recommendations a bit inconvenient? Sure, but they are a lot less inconvenient than dealing with a data breach or the loss of funds.

Data and money are transferred not just by computers, but by people using computers. The human element of each such system must be periodically reviewed and adjusted as needed to ensure two-factor authentication. Personnel must be trained to be aware of the types of traps that might be set for them and how to react to them.

Keep the horse outside the walls until you are sure there is no enemy hiding within.

KENNETH CITARELLA JD, MBA, CFE, CIPP/US

Senior Managing Director, Investigations and Cyber Forensics, Chief Privacy Officer

Ken Citarella is the Chief Privacy Officer for Guidepost Solutions. In that capacity he guides the international compliance efforts of the firm in its investigative, security consulting, due diligence and compliance consulting practices, including advising clients on how to create and maintain a privacy compliance program. An attorney and Certified Information Privacy Professional by the International Association of Privacy Professionals, Mr. Citarella was one of the earliest prosecutors in the nation involved in the investigation and prosecution of computer-based crime. The High Technology Crime Investigation Association bestowed its Lifetime Achievement Award on Mr. Citarella in 2011.