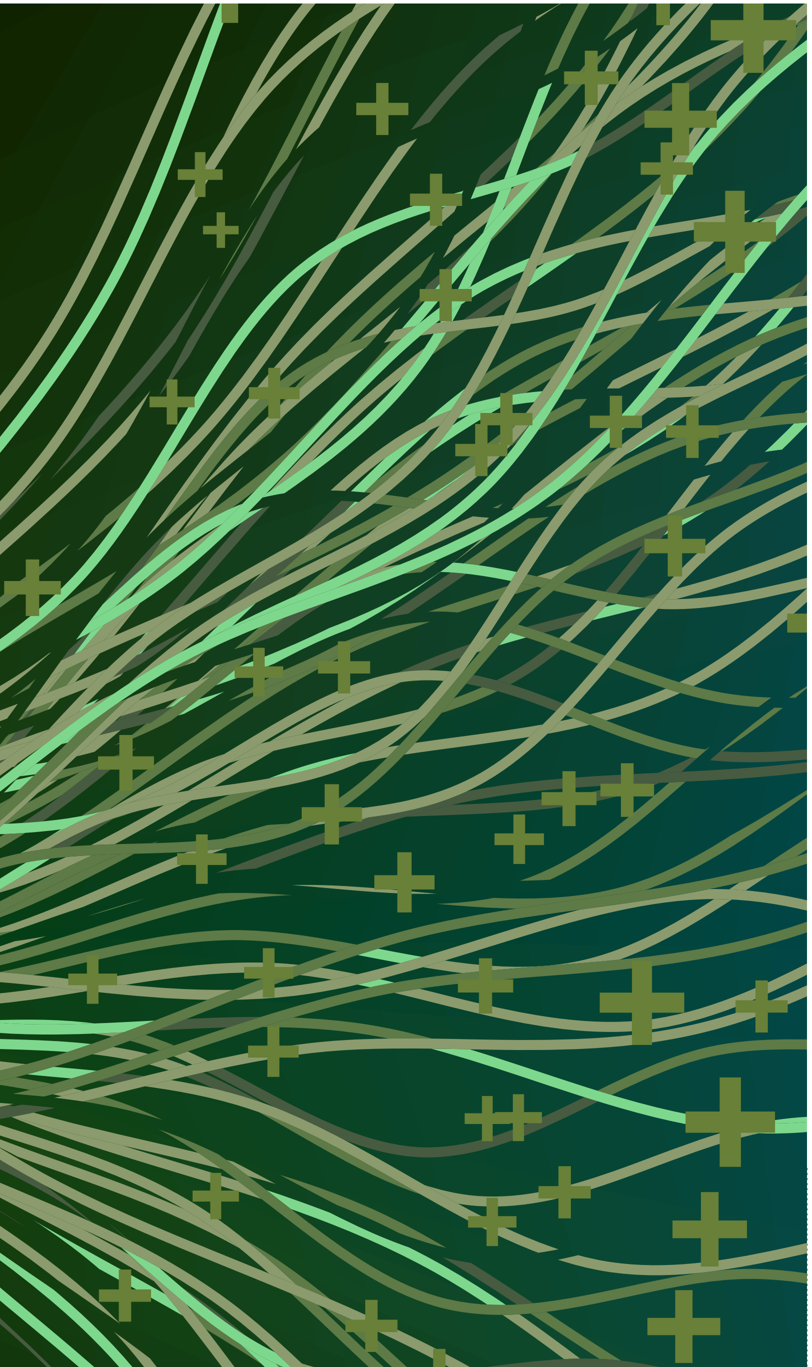

*E-Guide*

# BRING SPEAR PHISHING PROTECTION TO THE MASSES

TechTarget | SearchSecurity

**IN THIS EXPERT** tip, David Sherry describes how a combination of technical controls and user awareness training can help put a dent in phishers' attempts at spear phishing.

# BRING SPEAR PHISHING PROTECTION TO THE MASSES

*David Sherry*

Phishing attacks continue to be successful and are a genre of email attacks becoming more focused through spear phishing, which is a directed attack against a certain individual. We've already seen spear phishing used in high-profile incidents such as the attack on RSA, the security division of EMC Corp. and its SecurID two-factor authentication infrastructure. Specially crafted emails were sent to particular individuals at RSA in the hopes they would open the attached infected files and launch credential-stealing malware into the RSA network.

In order to counter this threat and ultimately keep data safe and compliance efforts in line, organizations need a mix of technical controls and awareness training of high-profile targets.

The term phishing was started by cybercriminals to indicate the act of tricking someone into revealing their private or sensitive information. These cybercriminals know if you ask a large number of people to provide such information, a small number will respond.

Home

Bring Spear Phishing Protection to the Masses

A majority of phishing is automated and perpetrated across botnets, and is considered to be an opportunistic attack, not a targeted one. However, the criminals also know that one successful attempt against a person of great wealth, responsibility or notoriety can be of great profit, and targeted spear phishing was born.

## ANATOMY OF THE SPEAR PHISHING ATTACK

While a mass phishing exercise may revolve around something that could be of interest to a large amount of users (such as banking or credit cards), spear phishing creates an attack that is specific to the intended victim. An email and webpage will still be built for the attack, but reconnaissance is necessary as prelude. The hacker will scour the Internet looking for information on a certain individual. Through public documents, chat rooms, social networks, blogs, and company websites, a digital dossier is developed about the target's interests, employment, responsibilities, charities, background, and family life. Therefore it's necessary to craft policies to address social media use and monitoring technology to watch content entering and leaving an organization that could put data at risk.

Home

Bring Spear Phishing Protection to the Masses

The construction phase comes next in a phishing attack, where the attacker will build an email and website specific to the individual to be attacked. Both the message and the landing page will contain information that is not only relevant to the victim (such as corporate information, economic or financial interests, or news about the person directly), but also is professional and legitimate looking in its presentation.  The message will be developed to be so believable that the intended victim will not think twice about responding. Users have to be wary about following links in suspicious email messages and about the information they input into an online form or website.

The harvesting begins when the victim clicks on a link or visits the webpage.  At this point, even if the victim is phishing aware and savvy enough to not provide personal or private information, malicious code can start in the background to scan and steal data from the victim’s computer (or gain access to the corporate network).  It then collects that data sends it to a command computer for analysis and use. From there, the attacker can sell the information, steal the identity, steal finances, seek to traverse the organization’s network, or attack the victim’s contacts.

## HOW TO PREVENT PHISHING ATTACKS: SPEAR PHISHING PREVENTION

To reduce the threat of spear phishing, security awareness and training to the right individuals is key. While a cybercriminal could use this type of attack on anyone, the data shows the targets are usually people of responsibility, notoriety or wealth. With this in mind, security professionals should address this issue with their organizations executives and leaders. Remember to also include executive assistants as well, as they may not only provide communications triage for their responsible executive, but could also be a target themselves.

Through the use of training memos, in-person demos and awareness campaigns, ensure the leaders of your organization know the risks of falling for a phishing attack, as well as the signs of an attack in process. Inform them to never click on a link in an email, chat session, blog or other medium. Eliminating this one action severely reduces the success of an spear phishing attack. They should also be instructed to be careful of unsolicited messages, especially ones containing public information about them. Vanity hacking (in which the victim falls prey to their ego) is on the rise, and is thought to be part of many recent high-profile breaches. Because of the time demands and responsibilities of the people you are training, remember to make the messages short, memorable and professional in nature.

Home

Bring Spear Phishing Protection to the Masses

Silly graphics and mascots are normally not effective in conveying security in the corporate boardroom.  Teach them the risks, as well as how to prevent phishing attacks.

Finally, while you raise the level of awareness of spear phishing for the end user, do not neglect the technical controls as well.  Ensure all antivirus, antimalware, personal firewalls and browser antiphishing controls are in place and up to date. A combination of phishing-aware users and a comprehensive technical strategy reduces the chance of a successful phishing attempt.

**AS CHIEF** information security officer of Brown University, David Sherry is charged with the development and maintenance of Brown's information technology security strategy, IT policies and best practices, security training and awareness programs, as well as ongoing risk assessment and compliance tasks. A CISSP and CISM, Sherry has 20 years of experience in information technology. He previously worked at Citizens Bank where he was vice president for enterprise identity and access management, providing leadership for compliance and security governance.

Home

Bring Spear Phishing Protection to the Masses

## FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

## WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.