Zenith American SOLUTIONS®

Future Focus

Z-MAIL

ZASSI

Zenith American Solutions Security Information

IN THIS ISSUE...

Email

Infiltration and Data Leaks

Malware infiltration and data leaks are more focused and persistent than ever before. Next generation threats are multi-phased and organized explicitly to bypass security defenses. End-users are the target. Impersonating end-user credentials is their goal. It only takes one end-user doing the wrong thing for an attacker to win. Staying informed is how we win:

- Attackers begin their efforts by searching public resources, social networks, identifying specific facts, individuals, associated friends, or acquaintances in line to their target.
- Crafted email is sent to their targeted end-users, typically carrying malicious code. Unknowing end-users activating this email unknowingly allow their credentials to be impersonated.
- Attackers employ the impersonated user ID, slithering off in search of other weaknesses, or their targeted information.
- Before leaving, attackers generally create easy reentry points to allow their return. At work or home – the attacker's methodology is the same.

Preventive actions include: (a) scrutinize email before acting; (b) be especially on guard for emails coming from unrecognized senders; (c) sender names not matching return email addresses; (d) messages asking to confirm information; (e) unordinary messages suggesting *urgent* responses; (f) messages written to upset you, targeting an emotional response, often threatening; (g) avoid clicking anywhere in the message body – even empty areas; (h) never enable the auto-preview reading pane on the Inbox (it can activate malicious code unintentionally); (i) avoid opening attachments from unknown senders; (j) remain suspect at all times!

Phishing

Phishing is an attempt to acquire interest or trust. This type of email is engineered to look pretty convincing! Generally masquerading as a trustworthy source. Most often originating from a popular site, bank, company, friend, or other reputable entity. Generally these messages are aimed to lure you into conveying information.

Attackers frequently use websites like Facebook, Twitter, Myspace and others to gain information about persons, even friends and family posts. While the attacker's motives appear seemingly trivial, these activities are done for their momentary gain. They do very well converting your collected information into cash. Personal information, even company information is quite valuable these days. Remember, little pieces of information collected over time equates to a big picture. This may be more than anyone would reasonably want to share.

Emotion

Emotions are a part of our lives, and dealing with them at work is unavoidable. Bringing our humanity to work includes happiness, excitement, enthusiasm, and laughter – as well as frustration, disappointment, anger, sadness, and worry. So when it comes to email, it's important to recognize factors that may inhibit our effective communications. Knowing that poorly chosen words or emotional distractions can miscommunicate intended messages. Unlike face-to-face interactions where we can hear the tone of voice, see facial expressions, body language, and synchronization to what we say or do – email relies upon the recipient's mood and perception. It's always a good practice to reread outgoing messages before sending. Always consider the possibility for misperception.

Encrypting Email

Personal information is becoming a high value target. Experts who monitor crime in cyberspace say, "America's medical records systems are flirting with disaster. A hack that exposes the medical and financial records of hundreds of thousands of patients is coming — it's only a matter of when". So, staying off the headlines means data encryption is our best friend. When it comes to email, always ensure protected health information (PHI) remains unusable, unreadable, or indecipherable to the unauthorized individual. While at work, encrypting email is easy – simply type "[phi]" in the subject line of your email. This action will encrypt your message, keeping both the individual's information and your communications safe.

These practices are very effective at work and at home. Protect yourself – our clients – and our company! Questions are always welcome: IT-InformationSecurity@Zenith-American.com