WHY TOTAL INBOX PROTECTION MATTERS

mortgagephish
FISH FOR BETTER INTERNAL SECURITY

Sara Cassidy Gray
scgray@mycloudstar.com

HISTORY AND ADOPTION EMAIL

Email as we know and understand it today stems from a mailbox system used at Massachusetts Institute of Technology in 1965. It wasn't until 1972 when Ray Tomlinson created email addresses, that computers were able to "talk" to each other in a new way. The late 80s brought about security concerns with "worms", designed to disrupt networks. Email bombs as denial of service attacks also made an unsettling entrance. Simultaneously, the base technique for phishing was utilized at this time. It wasn't until the mid-90s that the term was coined when a hacker was attempting to steal passwords and financial data.

In looking to the historical perspective of phishing, the May 2000 Love Bug hit email inboxes around the world. A simple message, "Kindly check the attached LOVELETTER coming from me" saw the disruption of 45 million Windows PCs. The Love Bug proved not only the scale of damage that could be accomplished by a phishing email, but how hackers play off of recipients' humanity and innate responses.

Year	Campaigns
2005	173,063
2006	268,126
2007	327,814
2008	335,965
2009	412,392
2010	313,517
2011	284,445
2012	320,081
2013	491,399
2014	704,178
2015	1,413,978

The 2010s saw a steep increase in the increase in both the frequency and total payouts to cybercriminals. Using the 2013 Target incident as an example, a subcontractor who had access to greater Target information fell victim of a phishing email. From that, 110 million customer and credit card records were stolen despite the subcontractor using anti-malware software; it wasn't enough.

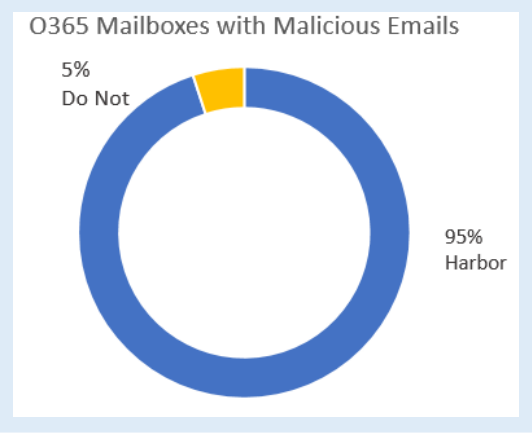
The nefarious actors within the internet found a foothold in email exploitation not long after the invention of the platform and their impact has gradually strengthened overtime to the measureable threat as we understand it today.

BY THE NUMBERS:

$12.5 billion dollars, globally, $150 million, in real estate wire fraud, these numbers relate to losses experienced from email compromise. That high level impact seems far removed from individual firms and agencies. Yet broken down, firms are, on average, losing $130,000 per successful attack; and trends are revealing that cost per attack is increasing, according to Stephen Dougherty, a financial fraud investigator with Firebird Analytical.

When it comes to actual reported complaints of business email compromise, the FBI received 351,937 complaints in 2018 and the Internet Crime Center (IC3) has reported 4.4 million. The FBI also advised: "It is worth noting that these are not national crime statistics, but just statistics from internet crimes reported to IC3. *The true figures will almost certainly be higher*."

Concurrently, over 70% of attacks stem from phishing emails. Once an email is compromised, a criminal can lie in wait, reading and gathering information to act at the opportune time to intercept wire transfers. Over 95% of Office 365 mailboxes harbor such malicious emails, according to Barracuda researchers.



All the while, phishing emails are becoming more difficult to detect from legitimate emails. From social engineering tactics to learning the business, hackers personalize 1 in 5 emails to the recipient, including their name.

Yet in spite of the statistics, agents continue to the believe in an inherent safety. This sense of safety is completely false. Those in the real estate industry or real estate adjacent industries are especially at risk, dealing with both large sums of money and remarkably vulnerable parties.

DNA OF A DATA BREACH

A data breach occurs via a usual but effective set of four steps.

1. Research: According to various researchers, this step has become increasingly more valuable to hackers overtime. Their ability to utilized public information, via victims' business website or social media allows for higher quality knowledge of internal goings-on, employees and ultimately, vulnerabilities.
2. Initial Contact: The initial contact itself is generally very noneventful for most data breach cases. In such cases, the hacker is looking for further vulnerabilities and weakness to design and set up for step 3.
3. Attack: Attacks can come in two forms, a network or social data breach. Social breaches especially rely on email credentials. A phishing email is sent; login credentials can be stolen.
4. Exfiltration: Once the hacker has access, they often lie in wait, sometimes for months to gain access to the most valuable data or to intercept the largest sum via wire fraud. At this point the attack is considered successful.

Historical data breaches from the Panama Papers to the 2013 Target incident followed similar steps, and often utilize adjacent trusted business and users as bait. Yet in those cases, end users are not necessarily the intended victim. Unique to real estate industries, they are.

A CULTURE OF SECURITY

When considering cybersecurity and the risks associated, finding a solution can seem easy. Yet the biggest hurdle for most agencies and businesses is cultural. An IT-lead security culture greatly improves security measure effectiveness. It is no longer an option to be passive toward security. Management must understand and support security measures but also provide necessary resources to create and support scalable solutions.

> **“As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture.”**
>
> **- Britney Hommertzheim, Director, Information Security, AMC Theatres**

Holding both management and employees accountable to security metrics anchors daily tasks toward IT goals. Creating weekly check-ins with IT, educational goals and programs and scaling up along with the business are great ways in which intangible ideals become pragmatic goals.

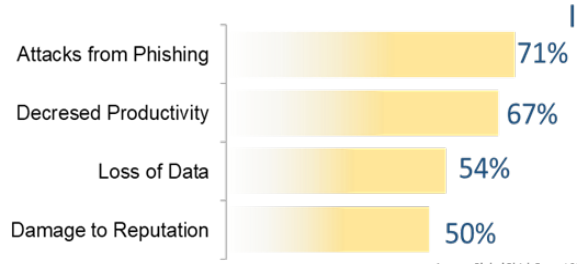
Risk assessments and reporting are easy and often underutilized ways to create the accountability. Direct reporting from IT leaders to management as well as sufficient delegation of authority also offers a way to shift culture toward greater security mindedness. Security must be cultural, go beyond simple compliance if it to offer real protection.

Learning the threats, risks and mitigation tactics of inbox protection and email security will continue to precede change. Information should act as a propellant to the change, spring-boarding that cultural shift to security. From that new vantage, will total inbox protection become the standard not just for individual businesses but industries overall.

WHY TOTAL INBOX PROTECTION MATTERS

75%
of Title Agents *do not* utilize Phishing Testing or Training
ALTA's Data & Analytics Work Group

IMPACT TO SMALL BUSINESSES



Avanan Global Phish Report 2019

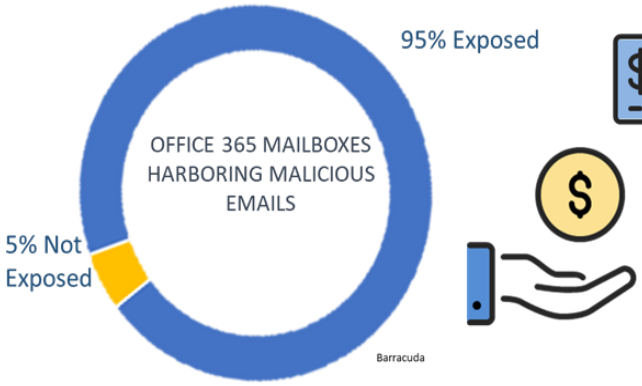
REPORTED GLOBAL LOSSES

$12.5 BILLION
EMAIL COMPROMISE

LOSSES IN REAL ESTATE

$150 MILLION
WIRE FRAUD ALONE

FBI Public Service Announcement I-071218-PSA



Barracuda

1 IN EVERY 5 PHISHING EMAILS IS PERSONALIZED TO THE RECIPIENT, INCLUDINING THEIR NAME

Agari Q2 2019 Report

4800 Spring Park Rd, Jacksonville, FL 32207
(800)340-5780