Email Security Threats and Trends

By | Kilausuria binti Abdullah & Sarah binti Abdul Rauf

Introduction

Email is an extremely popular method of communication. The ease of use and speed of communication via email make it attractive for business and personal use. Based on Wikipedia, email, or electronic mail, refers to a method of exchanging digital messages between people using digital devices such as computers and mobile phones.

In general, Internet email messages consist of two major sections, which are the message header and the message body. The email header is structured into fields such as From, To, CC, Subject, Date, and other information about the email. Simple Mail Transfer Protocol (SMTP) is a protocol used in the process of transporting email messages between systems by using message header fields.

Email Security

The popularity of email has made it a target of abuse by some people for their own benefit. Examples of email abuse are spam and phishing emails. When using email, users need to be aware there are threats involved. To avoid being scammed, users are advised to always apply best practices when using email and to become knowledgeable of newer issues with email.

Email Incident Statistics

Based from Cyber999 incident records, 657 incidents were reported regarding account compromise intrusions from 2012 to 2017(Q1). Below are the statistics on account compromise incidents reported for 2012-2017(Q1)

Year	Total Incidents by Year
2012	50
2013	153
2014	139
2015	119
2016	149
2017(Q1)	47

Table 1: Account compromise intrusions from 2012 to 2017(Q1)

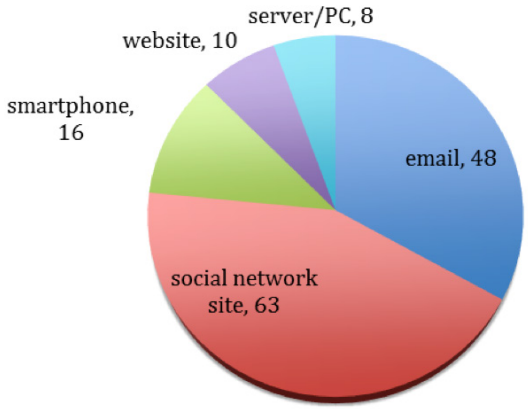


Figure 1: Account compromise intrusions in 2016 based on media used

Email Incident Trends

1. Spam Messages

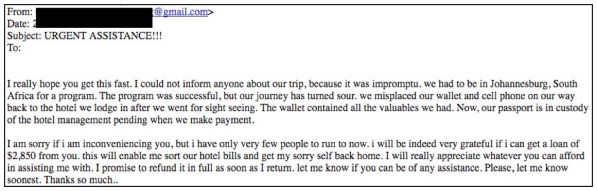
Spam email is the most common threat involving email. One of the spam messages trends is email-marketing campaigns. Email marketing campaigns are used because they deliver outstanding results for businesses. Spam email can also be used as a distribution mechanism for malware.

2. Email Phishing and Spear Phishing

Besides phishing emails that target banks, phishers have also created phishing emails and websites for other famous applications, organizations and email providers, such as PayPal, iTunes, Gmail, etc.

3. Scam Emails by Social Engineering

Hackers use victims' compromised email accounts to send scam emails to friends on the list of the compromised accounts. Scam emails can contain requests for help and money, claiming someone is supposedly in trouble.


From: [redacted]@gmail.com>
Date: [redacted]
Subject: URGENT ASSISTANCE!!!
To:

I really hope you get this fast. I could not inform anyone about our trip, because it was impromptu. we had to be in Johannesburg, South Africa for a program. The program was successful, but our journey has turned sour. we misplaced our wallet and cell phone on our way back to the hotel we lodge in after we went for sight seeing. The wallet contained all the valuables we had. Now, our passport is in custody of the hotel management pending when we make payment.

I am sorry if i am inconveniencing you, but i have only very few people to run to now. i will be indeed very grateful if i can get a loan of $2,850 from you. this will enable me sort our hotel bills and get my sorry self back home. I will really appreciate whatever you can afford in assisting me with. I promise to refund it in full as soon as I return. let me know if you can be of any assistance. Please, let me know soonest. Thanks so much..

Figure 2: Example of scam email

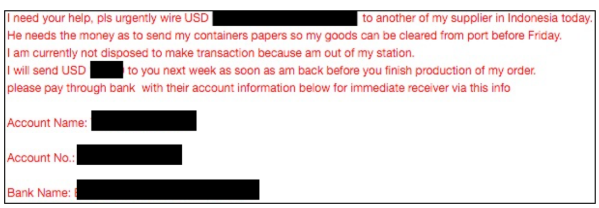
4. Spreading Malware

Another trend that is gaining momentum is email containing malware. The malware can spread via emails that contain links to infected sites or attachments that are infected with malware. When the user clicks on the link or opens the email attachment, the user's machine will be infected with malware. Some ransomware employs this method to spread. Ransomware is a type of malware that can lock users' computers or encrypt user files until ransom is paid.

5. Business Email Compromise (BEC)

Another common trend is Business Email Compromise (BEC). A variation of this is known as CEO fraud. In CEO fraud, cybercriminals might use hacked CEO emails to send impersonation emails to the finance manager or an employee in the finance department. This compromised email account is then used to trick the employee to transfer funds to an account controlled by the scammers.

Commercial Fraud is another BEC scheme that uses compromised email accounts to manipulate customers or suppliers to send funds to a fraudulent account. The most common method applied by cybercriminals to commit BEC fraud is email spoofing by social engineering (similar email address and similar domain).


I need your help, pls urgently wire USD [redacted] to another of my supplier in Indonesia today.
He needs the money as to send my containers papers so my goods can be cleared from port before Friday.
I am currently not disposed to make transaction because am out of my station.
I will send USD [redacted] to you next week as soon as am back before you finish production of my order.
please pay through bank with their account information below for immediate receiver via this info

Account Name: [redacted]

Account No.: [redacted]

Bank Name: [redacted]

Figure 3: Sample of commercial fraud email

6. Data Leakage and Business Disruption

Disgruntled ex-employees who previously managed the company email account may intentionally change the admin email username and password. The organization cannot directly reset the email account because that ex-employee who is the only one that knows the email server settings previously created it.

This type of threat can be minimized if the company has proper policies on staff termination and security procedures for handling company email.

Email Security Threat Mitigation

End-user email security best practices

- Never open attachments or click on links in email messages from unknown senders.
- Change passwords periodically and use best practices for creating strong passwords.
- Never share passwords with anyone, including co-workers.
- Try to send as little sensitive information as possible via email, and only send sensitive information to recipients who require it.
- Use spam filters and anti-virus software.
- When working remotely or on a personal device, use VPN software to access corporate email.
- Avoid accessing company email via public Wi-Fi connections.

By educating employees on email security and implementing proper measures to protect email, enterprises can mitigate many of the risks that come with email usage and prevent sensitive data loss or malware infections via email.

Enterprise Email Security Best Practices

There are multiple ways to secure email accounts. For enterprises, it is a two-pronged approach, encompassing employee education and comprehensive security protocols. Best practices for email security include:

- Engage employees in ongoing security education around email security risks and how to avoid falling victim to phishing attacks over email.

- Require employees to use strong passwords and mandate password changes periodically.
- Utilise email encryption to protect both email content and attachments.
- Implement security best practices for BYOD if your company allows employees to access corporate email on personal devices.
- Ensure that webmail applications are able to secure logins and use encryption.
- Implement scanners and other tools to scan messages and block emails containing malware or other malicious files before they reach your end users.
- Implement a data protection solution to identify sensitive data and prevent it from being lost via email.

Implementing defensive technology is important, but defending against attacks requires ongoing user awareness, training and proactively. For example, finance staff needs to be proactive when dealing with payments. They need to check email addresses carefully and if the request is suspicious, they should check via phone call with the person or institution that supposedly sent the email.

Another proactive measure is to use email encryption. Email encryption keeps messages and attachments illegible to unauthorized users. Be sure to deploy a solution that is not only secure but also easy to use. The easier the email encryption is for senders and recipients, the more likely it is to keep email secure.

In order to combat ransomware that spreads via email, employers need to educate employees on ransomware threats and the potential security risks affiliated with suspicious links and attachments. Employees must not click on unfamiliar links, especially shortened links, like bit.ly or owl.ly. Frequent and complete back-ups are also an important safeguard.

Conclusion

The best way to prevent private data from falling into the wrong hands is to take proactive action. Encryption is the best bet, keeping data safe even if your account is hacked or if your password simply falls into the wrong hands.

If the company refuses or has constraints with using encryption, some email protection can help against advanced email threats. It can protect against ransomware, business email compromise, spoofing, and phishing. Despite the best tools available to protect your company and you, users need to have basic knowledge about email security and understand the best email practices.

References

1. *https://en.wikipedia.org/wiki/Email*
2. *http://write.flossmanuals.net/basic-internet-security/introduction-to-e-mail-safety/*
3. *https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/infosec-guide-email-threats*
4. *http://www.focus.net.nz/blog/category/general/email-security-best-practices*
5. *https://www.cambridgenetwork.co.uk/news/huge-rise-in-cyber-attacks-as-criminals-start-to-target-smal3964/?*
6. *https://www.zixcorp.com/resources/blog/january-2017/email-security-threats-to-watch-in-2017*
7. *http://library.ahima.org/doc?oid=99319#.WQA6RR0lFn4*