ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

An Introduction of the RIST Framework on Information Security Awareness Practices in the Current Information Age

Kudakwashe Zvarevashe[1], Tinotenda Zwavashe[2], Cephas Mawere[3]

M Tech Student, Dept of CSE, Jawaharlal Nehru Technological University, Hyderabad, India[1]

M Tech Student, Dept of ECE, Jawaharlal Nehru Technological University, Hyderabad, India[2]

M Tech Student, Dept of Bioinformatics, Jawaharlal Nehru Technological University, Hyderabad, India[3]

ABSTRACT: Information Security awareness has been an important vehicle in the acknowledgement, training and exposure of Information threats, vulnerabilities and attacks. This has brought about a large number of training programs and technical researches in order to make people aware of the dangers that haunt them in this computing world. The emergence of new technologies has had a twofold effect on the people that use them. Most technologies have brought a significant improvement as far as availability, processing and storage is concerned. However, the issue of security has been an obstacle in the full acceptance of the technologies and also user appreciation. Therefore this paper discusses the issues that are recently impacting Information Security Awareness in line with the current technological trends. It also aims at providing the best ways of alerting people on how to implement Information security measures in this current technological world and thereby building confidence in users. The paper will also delve into issues like social engineering, email attacks, Smartphone/ mobile attacks and social networks confidentiality.

***KEYWORDS*:** Information security awareness, RIST, threats, vulnerabilities, attacks, social engineering, smartphone, social networks, confidentiality.

I. INTRODUCTION

Information security has been discussed in many for a both in academia and industry, Today the information security challenges we are faced with are ubiquitous, and highly dynamic. The solutions we devise to solve today's information security services will not work on tomorrow's security problems. This scenario results in more information security practitioners also gearing up and matching the dynamism and ubiquity of the security problems. As much work having been done both in Academia and Industry in securing the large volumes of information being generated every day. One piece of the information security puzzle is still lagging behind. Information security awareness has not been as dynamic as the security challenges and their solutions. Any chain is as strong as its weakest link, in the case of Information security, the user is the weakest link. Users have not been provided with on timely security awareness programs to give them an edge over attackers.

II. SOCIAL NETWORKS

In [2] online criminals and spammers are no longer interested in attacking emails. Instead they have formulated several attack vectors on Social Networks. This is because the social media is presenting them with several options and the flexibility to steal people's identities or personal information as well as creating avenues to install various forms of malware.

Social media provides two behaviours that are very useful for criminals and these are social proofing and sharing. Social proofing is a psychological mechanism that tempts and convinces people to do things simply because their friends are doing it. For example if you get a message from your friend on Facebook you are inclined to click it simply because it is from your trusted friend. Sharing is one of the purposes of Social Networks. It is indeed a fibre that makes us social beings. People share personal information such as their birthdays, addresses, relationship status, contact

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

details etc. This information can then be used by criminals to steal identities. For example a social media profile may contain clues to security questions a hacker could reset the user's account and use it as if it were his.
Research firm, Javelin Strategy & Research, examined the way people behave in popular social networking sites. It found that those with public profiles were more than likely to share specific personal details like:

- Birthday (68%)
- High school (63%)
- Phone number (18%)
- Pet's name (12%)

Note that prospective employers rely on these details to verify future employees' identities. Letting these fall into the wrong hands can therefore severely compromise your identity.

In this information age that we are leaving in a lot of people are spending most of their time on the internet and a large part of it is spent on Social Network sites like Facebook. Most people access the social network websites using mobile devices especially smartphones and this presents online criminals with a wonderful opportunity to perform their criminal activities.

According to Symantec, the top five social network criminal acts are :

- Fake Offering
- Manual Sharing
- Likejacking
- Fake Plug-in
- Copy and Paste

Fig. 1.0 Symantec Social Media Attacks in 2013

1) Fake Offering: These scams invite social network users to join a fake event or group with incentives such as free gift cards. Joining often requires the user to share credentials with the attacker or send a text to a premium rate number.

2) Manual Sharing Scams: These rely on victims to actually do the hard work of sharing the scam by presenting them with intriguing videos, fake offers or messages that they share with their friends (Fig. 2.0).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Fig. 2.0 Illustration of Manual Sharing scam from Facebook

3) Likejacking : Using fake "*Like*" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, spreading the attack.

4) Fake Plug-in Scams: Users are tricked into downloading fake browser extensions on their machines. Rogue browser extensions can pose like legitimate extensions but when installed can steal sensitive information from the infected machine.

5) Copy and Paste Scams: Users are invited to paste malicious JavaScript code directly into their browser's.
To prevent oneself from the various Social network attacks the following measures can be very useful:

1. Be wary of clicking shortened links from unknown accounts. Always try and verify shortened links before you actually click them. Twitter's web client allows you to preview shortened links by hovering your cursor over them.

2. Only befriend or follow people you've met in real life or whose accounts you've verified. Never follow anyone you may not know in real life or have no mutual friends with. If you must follow celebrities or public identities, see if their accounts have first been verified by the social networks they're in.

3. Read the security settings of the site you are signing up for. Social networking sites are aware of the threats that cybercriminals spread on their networks. Most have even rolled out built-in security features to help combat threats. Explore these fully and enable them as soon as you can.

4. Use hard-to-guess passwords. Use phrases of more than three words. They're much easier to remember than complicated words formed using a combination of letters, numbers, and special characters.

5. Privacy is a commodity, don't waste it. If you're worried about anything on your personal pages ending up in strangers' hands, set your profile to "Private." That way, only your trusted contacts can see them

6. Group your contacts. This helps limit what each group of contacts see on your personal pages.

III. EMAIL SECURITY

E-mails are one of a major communication methods for official data exchange. As a result attackers have of late developed several ways of duping e-mail users and the users have suffered devastating loses at the hands of these attacks. Generally lack of knowledge on how to combat suspicious emails has been the main cause of these loses.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Attacks on email services can have damages ranging from denial of access to email to substantial financial loss or even magnified loses. Generally email attacks come in three main forms which are:

i. Spam
ii. Phishing
iii. Viruses

These three can be interlinked such that the existence of one can bring in the other threat(s). One of the primary attacks on email security is email spam or junk emails. By clicking on links associated with spam email the links can lead to phishing websites and / or contain malware or virus hosting websites. Malware can also be contained in the spam itself in the form of scripts or executable file attachments. Thus phishing will provide a link to a website which is meant to obtain one's personal data. The phishers' main targets are bank customers and online payment services. It is estimated that between May 2004 and May 2005 computer users totalling 1.2 million in the USA suffered losses and damages to phishing, totalling approximately $929 million.

Recently huge efforts have been made to strengthen email security by fighting spam. It can be noted that spam rate declined from 75% in 2011 to 69 % of all email in 2012 with the takedowns in botnets continuing in 2012. Although there has been a significant decrease in spam the attackers have tried to remain in business by using other alternative ways like social networking. Social networks can be a profitable source of personal information to the attackers. Phishers are targeting these so that they get personal details that can be used in identity theft. Experiments show a phishing success rate of over 70% on social networks.

Collection of metadata can also be used as a way of collecting personal information of email users. This capability has been proven at MIT's Media Lab in their Immersion Experiment. This visual data experiment allows one to enter their Gmail address and brings out the network of people one is connected to via email and how this network evolves over time. Although the experiment does not have access to email bodies it has access to metadata which includes headers like "to:", "from:" "Cc:" and time of sending or receiving the email. The relationship one has with the people in the network can also be revealed. This, therefore, can be used as a destructive tool by attackers to monitor the communication behaviour of their target. The diagram shows some form of network analysis for a certain user for a period of about 3 years as depicted by MIT's Immersion Experiment (Fig. 3.0).

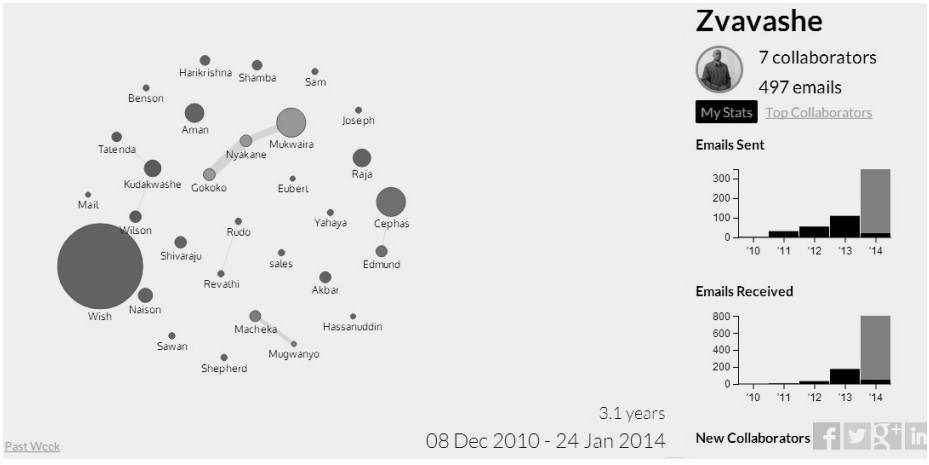

Fig. 3.0 Illustration of Email nodes and links from a single Gmail account

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

As such email users need to be educated on how to avoid receiving spam emails and also how to deal with the few which still get access to their emails. The importance of spam filtering should be communicated to the ordinary users (mainly those who don't have much knowledge on Email and computer security) and how they should deal with suspicious emails. This incorporates training people how to recognize phishing attempts, how they can modify their browsing habits, use of anti phishing software and how to use specialized filters, as stated earlier on, to reduce number of phishing emails that reach their inbox.

IV. MOBILE THREATS

Lost mobile devices continue to pose a major security problem with malicious apps and social media threats emerging as the dominant security issues. For instance, mobile malware escalated last year with increasing numbers of internet connected mobile devices[1][4]. Most of these devices are smartphones which makes them attractive to criminals. According to Gartner, Android currently has a 72 percent market share with Apple iOS as distant second with 14 percent [5].
Most mobile phone attacks have however continued increased in form of Android threats, privacy leaks and premium number fraud. Last year alone Android threats were more common in Europe and the United States [4]. Privacy leaks that reveal personal information have gone as far as transmitting the owner's location following the release of the surveillance software to smartphones [6][10]. Symantec, one mobile botnet observed that fake mobile apps were being used to infect users at the same time generating money from the mobile malware [7].

One interesting case is that of German university researchers who found that 8 percent of 13, 500 apps downloaded on Google play were vulnerable to man-in-the-middle attacks. Meanwhile about 40 percent enabled the researchers to capture credentials for bank accounts, American Express, Paypal and social networking sites like Facebook, Google and Yahoo, remote control servers and IBM Sametime, among others [1]. Additionally, cyber criminals have began using Android botnets to link mobile networks to send out unwanted emails or text messages [8], an adapted technique from PCs.

Last year trusted sites of apps were increasingly breached as malicious apps appeared more frequently. The risk of malware infecting a mobile device has been fuelled by a technique that helps users pirate mobile apps. Websense Security Labs reviewed permission requirements of malicious apps in their library against the permissions of legitimate apps currently available. They found out that 82 percent of malicious apps send, receive, read or write SMS messages, something which very few legitimate apps require any SMS permissions [1].
Also, one in eight malicious apps required RECEIVE_WAP_PUSH permission, a rarely requirement by legitimate apps too. Moreover, one in 10 malicious apps asked for permission to install other apps- another rarity among legitimate apps [1]. Thus, users should carefully examine apps that request any of these permissions to see if the permission request makes sense. At the same time users ought to know how legitimate apps behave in order to discern malicious apps. For instance, many legitimate apps are now requiring web-access permissions to support a social media feature and put ads in free apps, among other things [1].

Nonetheless, legitimate apps are no longer immune to malware attacks. In 2012, rogue software masqueraded as popular games on the Google Play market, having bypassed Google's automated screening process [9]. Now, businesses are increasingly allowing staff to use their smartphones for work, even subsidizing their purchase, in the hope of reducing costs. Since mobile devices lack security features like encryption, access control, and manageability, such businesses are now at a greater risk to lose their money via cyber fraud and spamming [4].

Android dominates the malware landscape with 97 percent of new threats making Android users vulnerable to a whole host of threats. This continues to increase as the Android platform provides the option to install apps from unofficial markets by simply changing settings in the operating system without an exploit against the threat in the software. Symantec recorded at least 3 906 different mobile variants of threats for 2013 in the Android market [4]. As a way of improving security, Google added a feature in Android version 4.x to allow users to block any particular app from pushing notifications into the status bar. This came in response to feedback from users of older versions, annoyed by ad platforms that push notifications to the status bar.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Google also added a feature in Android 4.2 to prompt the user to confirm sending the threatening premium text messages such as Android.Opfake, Android.Premium, Android.Positmob, and Android.Rufraud. This can assist users protect their mobiles from malicious attacks. By the beginning of 2013, Android 4.2 devices account only for a small percentage at around 10 percent market penetration [4].

However, the Android ecosystem makes it difficult to keep everyone up to date. Google released the official platform that works out of the box only on Nexus devices—Google's own branded device. From there each manufacturer modifies and releases its own platform, which is in turn picked up by mobile network operators who also customize those platforms [4]. This makes it impossible for any change coming from Google to be quickly available to all in-field devices. Any change to the platform requires thorough testing by each manufacturer and then each operator, all adding to the time needed to reach users.

The presence of many device models also multiplies the amount of resources all these companies have to allocate for each update. Hence, infrequently updates are released or in some cases there are no updates for older devices. For most exploits in the OS, Google released quick fixes. However, users still had long waits before they received the fix from their network operators. Some exploits are not in the original OS itself but in the custom modifications made by manufacturers, such as the exploit for Samsung models that appeared in 2012 [4].
Samsung (in the case of upgrading firmware for S3 and Note 2 smartphones) was quick to fix it, but the fix still had to propagate through network operators to reach users. Tighter control from Google over the platform can solve some of the "fragmentation" issues, but this could affect the relationship it has with manufacturers [4]. A cut-off point for older Android users could help to mitigate the risk, but it is usually the manufacturers that do this.
Meanwhile, it has been observed that smartphones users spend most of their time on internet browsing (24.81 minutes per day) followed by 17.49 minutes of social networking, 15.64 minutes of playing music, 14.44 minutes of gaming and 12.13 minutes of making a phone call. According to this information, smartphone users spend almost 50 percent more time using their mobiles for social networking than phone calls [2]. This has heightened the social risk that comes with using mobile phones.
Data also shows that 73.6 percent of iPhone users actively connect to Facebook using Facebook app for iPhone, and the Android version of the app has a 30 percent higher penetration rate [3]. As a result, all Social Web associated threats also pose a threat to mobile devices.

V. THE RIST(RESEARCH, INFORM, SELECT AND TRAIN) FRAMEWORK

With all this being said, we have discovered that something is missing in implementing the Information Security Awareness practices. Big companies are conducting a lot of researches and they are exposing a lot of hidden threats and vulnerabilities in the instruments that support most Social media. However, people have not been fully made aware of how they can protect their information or identities. In fact , the exposure of these threats has induced some technological fear in the users and potential users of Social Networks. As if that is not enough, the exposure of some of these threats is only limited to a number of scholars or researchers in the relevant fields while the bigger fraction of naive users are left vulnerable.

Training programs should cover a bigger area than what is being currently covered. Workshops are being conducted in major universities but little is being done in the workplace. Nurses, policemen, judges auto-drivers and many different workers are also users of the social media and they deserve to be made aware of the vulnerabilities they face on social networks. Therefore we have designed the RIST(Research Inform Scrutinize and Train) framework that can be used in implementing Information Security Awareness practices (Fig. 4.0).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

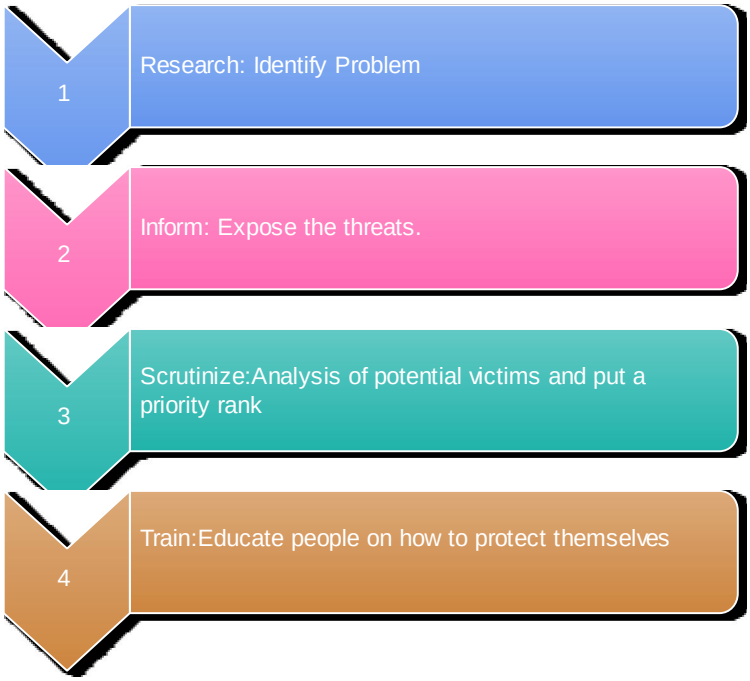

Fig. 4.0: The RIST Framework

The RIT framework consists of three phases which include researching, informing and training.

1. Research: In this phase we expect problem identification to take place and this may include the identification of the threats , vulnerabilities and attacks on a particular platform. This is what is currently being spear headed by the leading big security companies like Symantec, Websense and many more.
2. Inform: This is the phase whereby the information about these threats based on the research findings is disseminated and exposed to the public. This may include publication of the findings through white papers, technological magazines, academic publications etc.
3. Scrutinize: This is the phase whereby the threats , vulnerabilities and attacks identified will be carefully analyzed so as to build a taxonomy of the threat levels based on the potential victims. This will enable all classes of people to be targeted for the information security awareness programme.
4. Train: The training phase will then consist of the educating of the users and potential users of the technology involved. This may include a plan designed in the Scrutinize phase which classifies people according to their jobs or vulnerability. This is where the coverage of the training program is expected to increase so as to empower people with the knowledge about the threats, vulnerabilities and the possible solutions to these problems.

VI. SUMMARY AND CONCLUSION

Information security awareness has been going on for some time at big institutions like Universities but unfortunately the common like auto-drivers, bus conductors and many more have been left out. This has been happening due to the lack of a proper information awareness practice framework that will help in making information security accessible to all kinds of people. For our future work ,we are going to introduce the RIST Framework to a small community and make statistical comparisons with an identical community which will not be making use of the framework.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

REFERENCES

1. Websense 2013 Security Predictions, Jan. 2014, http://www.websense.com\2013predictions
2. FactsMark Authority, July 24, 2012, http://www.factsmark.com/the-call-usage-decline-in-smartphones/
3. TechCrunch- Jan. 4, 2013- "Facebook Mobile User Counts Revealed: 192M Android, 174M iPhone, 48M iPad, 56M Messenger," http: techcrunch.com/2013/01/04/how-many-mobile-users-does-facebook-have
4. Symantec Corporation, Internet Security Threat Report, April 2013, "Social Networking, Mobile, and the Cloud," 18
5. http://www.gartner.com/it/page.jsp?id=2237315.
6. http://www.symantec.com/connect/blogs/androidbmaster-million-dollar-mobile-botnet.
7. http://news.cnet.com/8301-1009_3-57470729-83/malware-went-undiscovered-for-weeks-on-google-play.

http://www.nytimes.com/2012/08/31/technology/finspy-software-is-trackingpolitical-dissidents.html?_r=1.

BIOGRAPHY

Kudakwashe Zvarevashe: Attained his BSc degree in Information Systems at MSU, Zimbabwe in 2010. He is currently doing M Tech IT final year at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of big data, information security, cloud computing and web services.

Tinotenda Zwavashe: Attained his B.Eng Degree in ECE from NUST, Zimbabwe in 2010. Currently he is studying towards M.Tech Embedded Systems at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of Network and security, wireless and sensor networks, Microcontroller based design and Real Time Operating Systems.

Cephas Mawere: Attained his B.Tech degree in Biotechnology at Chinhoyi University of Technology, Zimbabwe in 2010. He is currently doing M Tech Bioinformatics final year at JNTUH, India. He is a HIT staff development research fellow. His research interests are in the area of Bioinformatics ,Information Security and High Performance Computing.