SÛNNET BESKERMING

PROFESSIONAL NETWORKING SITES & PHISHING

SPORTS PHISHING FOR BEGINNERS

CARL JONGSMA

LEAD RESEARCHER

Table of Contents

Professional Networking Sites & Phishing

1. Introduction

This is a document that is many things to many people. For the technical reader, there is a detailed break down of what appears to be a new set of techniques being employed by phishers who are targeting users on Professional / business networking sites.

For the non-technical reader, this report provides a walkthrough of a scam attempt that they are likely to encounter in the future when logged into Professional / business networking sites, and it will help them identify potentially risky situations.

To achieve this balance, a detailed Glossary is attached which will allow the non-technical reader to understand the scope and relevance of the data provided even if certain concepts have not previously been encountered. If a reader needs more information about what phishing is, there aree plenty of worthwhile resources available online, and Sûnnet Beskerming will be more than happy to deal with any new clients seeking more detailed guidance.

2. Using This Document - Your Rights

How do we want you to read and use this document? Print it out, share it around, forward it to friends, family, colleagues. So long as you do not modify this document in any way, and attribute its source correctly, you have the right to use it as you see fit.

The information presented in this document is for information purposes only and Sûnnet Beskerming accepts no liability for damages that may be encountered due to the misapplication of that information. If you are contacted by the *real* Prince Ubuntu of Nigeria and miss out on your chance for millions of dollars as a result, *c'est la vie*.

3. Background & Initial Interaction

Sûnnet Beskerming's Professional Management guidelines recommend that employees maintain active membership of at least one Professional networking site, in an effort to improve their future employability and current net worth as an employee.

One of the more active sites that we use is Ecademy[1], based in England. With more than 100,000 members[2], the site provides access to a broad range of business professionals, with a distinct bias towards European contacts.

As with similar sites, Ecademy provides a means for users to contact each other via an onsite messaging system that is like an internal email system. So long as a user hasn't hidden their account from view, any other user may, depending on their account type, contact them and establish communication.

On January 21, a Sûnnet Beskerming employee (Carl Jongsma) received a message (Figure 3) via this system from somebody claiming to be Abdulla Qassem, a banker with the Emirates Banking group in the United Arab Emirates. The site profile (Figure 1) for the user was a loose match for the corporate profile of the real Abdulla Qassem (Figure 2), which was checked as a matter of routine. The Ecademy Abdulla Qassem provided a reasonable explanation for seeking out Carl and making contact, so a response was created (Figure 4). A more detailed message was then sent to Carl, at which stage the full exchange was handed over to Sûnnet Beskerming for investigation and continuation of contact. This was done transparently so as not to spook the user on the other end of the message.

Up to this point, everything still seems somewhat legitimate. There are a couple of concerning elements which suggest a 419 type scam in the building, but nothing that would concern the average user. Sûnnet Beskerming originally dismissed most of the elements as being language difficulties for someone where English was not their primary language, but remained cautious until more evidence could be gathered.

One of the problems of a temporary account on various networking sites is that they can disappear very quickly, so Sûnnet Beskerming moved to establish two-way email communication as a matter of course. The primary reason for doing so was to allow for more efficient data gathering and processing, particularly evidence that would confirm or dismiss the suspicions held about the Ecademy Abdulla Qassem.

---

[1] http://www.ecademy.com

[2] http://www.ecademy.com/node.php?id=74845

4. Investigation

Even though we had already done a little bit of background investigation work while trying to verify the existence of Abdulla Qassem, we were confident of a phish in the building when we moved to direct emails for communication. As a result, we reinvestigated every possible piece of information and communication that had been passed between us in an effort to find firm evidence of identity spoofing and what the person who we were communicating with was after (phishing, 419, or spam).

Will the Real Abdulla Qassem Please Step Forward

Not only did we need to validate the identity of the Ecademy Abulla Qassem, but we also needed to develop a basic trust level based on how different information sources presented data on Abdulla Qassem. Relatively quickly we became suspicious that the Ecademy profile (Figure 1) was an almost word-for-word match for a corporate profile provided on the Emirates Banking Group website (Figure 2). The significant discrepancy between the supplied email addresses and what could be found via major search engines also was a cause for initial concern.

Figure 1 - The Ecademy account as it was

Figure 2 - The real Abdulla Qassem

As we became more certain that the Ecademy Abdulla Qassem was not legitimate, we began to search for the sources used to create the cloned account (with the already-identified corporate page being the primary source).

Although the real Abdulla Qassem did not reply to any emails sent to accounts known to be linked to him, the failure to mention this side channel contact was another element of concern against the Ecademy user.

Previous Phishing

Satisfied that Abdulla Qassem is a real person, but still dubious about the true identity of the individual who had contacted us via Ecademy and email, Sûnnet Beskerming set out to uncover whether anybody else had encountered spam or phishing attempts from somebody claiming to be Abdulla Qassem.

What was discovered was a single report[3] from mid-November, 2006, where somebody claiming to be Abdulla Qassem had sent out a mass email phish, only this time claiming control of $17.5 million USD belonging to one of the victims of America Airlines Flight 587, which crashed in November 2001.

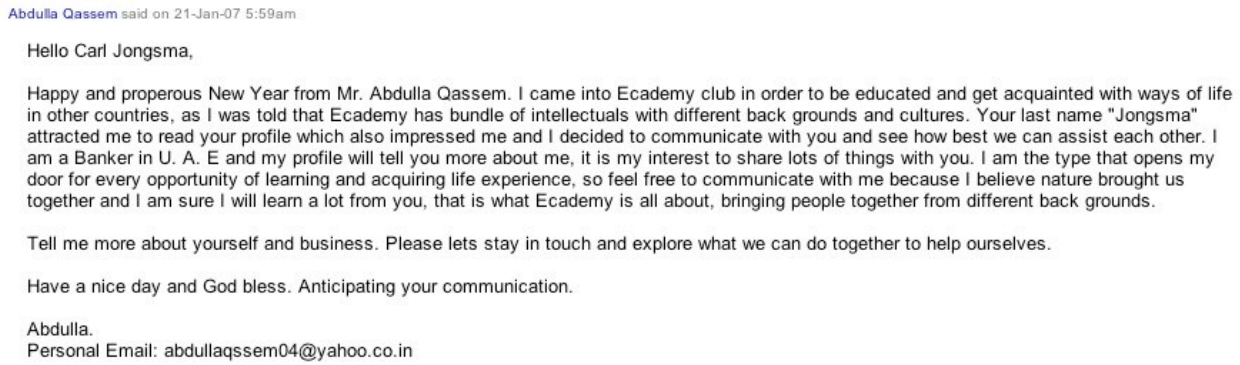
[3] http://www.joewein.net/419/emails/2006-11/16/859734.1.htm

Points of note to come from this email sample were:

- The email address used was yet another of the form 'abdullaqassem*nn*', where *nn* is a number, making use of free email accounts. This is not one of the separately identified legitimate email addresses for Abdulla Qassem, and does not match any pattern associated with the legitimate addresses.
- The email was still signed 'Mr. Abdulla Qassem'.
- The phisher had no problems identifying themselves as a Middle-Eastern banker who was responsible as the account holder for a deceased account, which showed parallels to the data being supplied in our discussions.

Interaction

Beginning with the initial contact via Ecademy, Sûnnet Beskerming kept a record of all communication that passed between us and the individual(s) claiming to be Abdulla Qassem. Communication through Ecademy is of limited forensic interest when trying to determine the actual location of the user, however the content is extremely valuable for building a picture of how future attacks may emerge.



Abdulla Qassem said on 21-Jan-07 5:59am

Hello Carl Jongsma,

Happy and properous New Year from Mr. Abdulla Qassem. I came into Ecademy club in order to be educated and get acquainted with ways of life in other countries, as I was told that Ecademy has bundle of intellectuals with different back grounds and cultures. Your last name "Jongsma" attracted me to read your profile which also impressed me and I decided to communicate with you and see how best we can assist each other. I am a Banker in U. A. E and my profile will tell you more about me, it is my interest to share lots of things with you. I am the type that opens my door for every opportunity of learning and acquiring life experience, so feel free to communicate with me because I believe nature brought us together and I am sure I will learn a lot from you, that is what Ecademy is all about, bringing people together from different back grounds.

Tell me more about yourself and business. Please lets stay in touch and explore what we can do together to help ourselves.

Have a nice day and God bless. Anticipating your communication.

Abdulla.
Personal Email: abdullaqssem04@yahoo.co.in

Figure 3 - Initial contact

The first contact from the user (Figure 3) appears fairly straight forward. There are some obvious difficulties of English expression, though this can be attributed to the user not speaking English as their first language. Reasoning given for the initial contact (based on a search of surname, which is recorded in Carl's user profile) is a legitimate means of finding accounts through the Ecademy site. Provision of a personal email address is also not unusual, especially as the user is on a temporary 'Guest' account, valid for 14 days. If they decide not to renew their account, then the email address supplied is a safety mechanism. Immediately, a spelling mistake in the address is noticed (and repeated later), and the first doubt about the legitimacy of the account is raised. Why would such a high ranking executive be using a webmail account as a primary contact, especially given the nature of their tertiary education and current business interests?

22-Jan-07 5:19am

Hello Abdulla,

Thank you for making the time to make contact with me. A happy and prosperous New Year to you, too. I would strongly recommend that you take up the offer of becoming a regular Ecademy member, it provides a wealth of useful resources that make it well worth the ongoing fee. Should you decide not to stay with Ecademy, I can be reached via email (info@beskerming.com).

I thank you for the kind words on my profile. I found your profile to be quite interesting, as well as the other information available about you via your Bank's online site. I am very interested in investigating what possible working relationships we can establish between our companies. A good starting point in order to find out more about what I, and my company, can provide, is our website http://www.beskerming.com.

Put simply, we provide a set of unmatched Information Security and Intelligence services, providing protection to people, companies, and their assets. You might be interested to know that we also have services designed specifically for high net worth individuals, helping them protect their position and assets (something that may be of use to you or your clients).

Once you have had the chance to look over our site and the material that can be downloaded, I will be able to provide you with more information about what we can do for you.

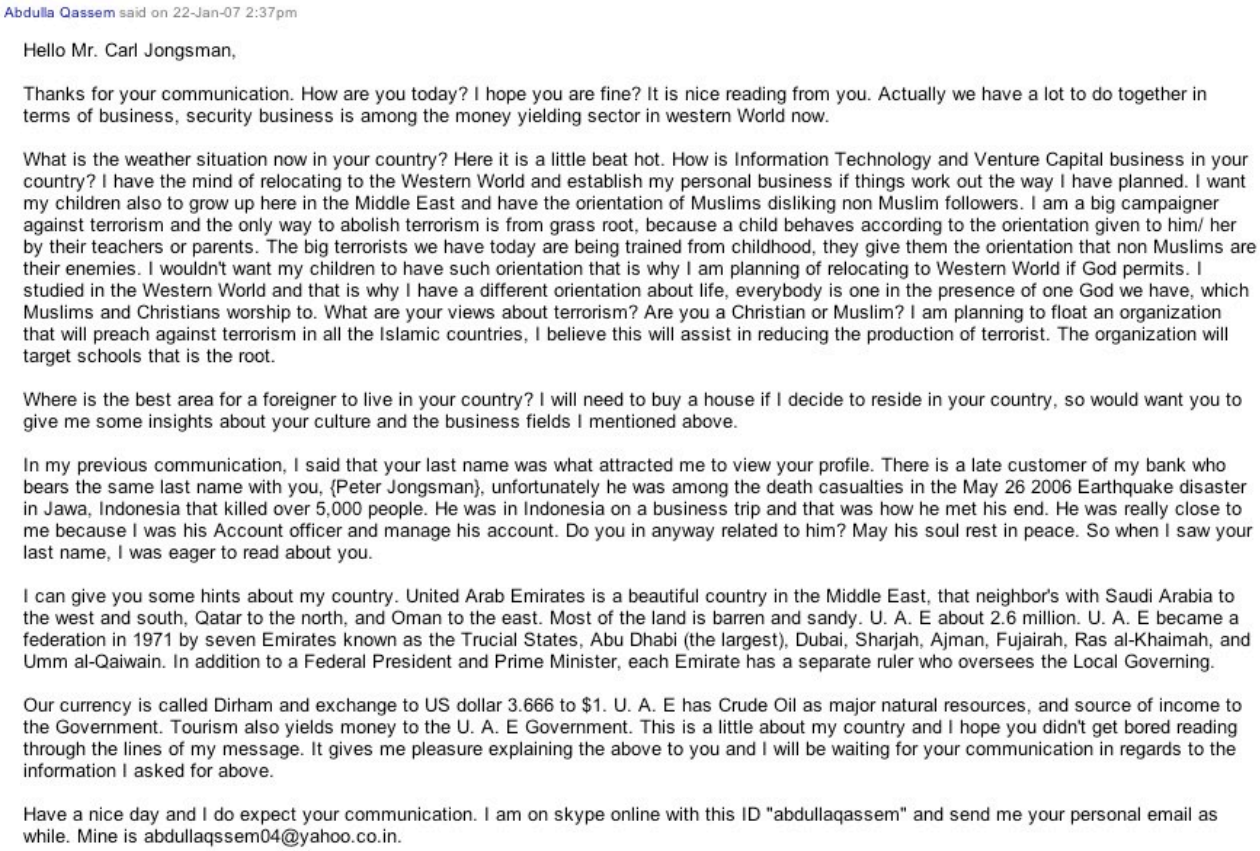
Regards,

Carl Jongsma
info@beskerming.com

Figure 4 - A response

Giving the benefit of doubt to the Ecademy Abdulla Qassem, Carl responds with a neutral, but friendly reply (Figure 4). At this point in the relationship, there is nothing to suggest anything taking place other than two business people establishing a working relationship.

It should be noted that at this stage it is not possible to determine the legitimacy of the Ecademy Abdulla Qassem. Assumptions about the level of functional English required to complete a tertiary degree at a small North American University can not be verified. The use of a free webmail account as a primary personal address, instead of one of the corporate accounts available to Abdulla Qassem is more of a concern, especially given the apparent spelling mistake in the account name. Email later sent to this address (spelled exactly as per the message) will show that 'abdullaqssem04' is not a legitimate account with yahoo.co.in, though 'abdullaqassem04' is. Failure to provide an Etisalat (eCompany), or a Sahm Net [the two possible ISPs in the UAE] email address is a lingering question mark.



Abdulla Qassem said on 22-Jan-07 2:37pm

Hello Mr. Carl Jongsman,

Thanks for your communication. How are you today? I hope you are fine? It is nice reading from you. Actually we have a lot to do together in terms of business, security business is among the money yielding sector in western World now.

What is the weather situation now in your country? Here it is a little beat hot. How is Information Technology and Venture Capital business in your country? I have the mind of relocating to the Western World and establish my personal business if things work out the way I have planned. I want my children also to grow up here in the Middle East and have the orientation of Muslims disliking non Muslim followers. I am a big campaigner against terrorism and the only way to abolish terrorism is from grass root, because a child behaves according to the orientation given to him/ her by their teachers or parents. The big terrorists we have today are being trained from childhood, they give them the orientation that non Muslims are their enemies. I wouldn't want my children to have such orientation that is why I am planning of relocating to Western World if God permits. I studied in the Western World and that is why I have a different orientation about life, everybody is one in the presence of one God we have, which Muslims and Christians worship to. What are your views about terrorism? Are you a Christian or Muslim? I am planning to float an organization that will preach against terrorism in all the Islamic countries, I believe this will assist in reducing the production of terrorist. The organization will target schools that is the root.

Where is the best area for a foreigner to live in your country? I will need to buy a house if I decide to reside in your country, so would want you to give me some insights about your culture and the business fields I mentioned above.

In my previous communication, I said that your last name was what attracted me to view your profile. There is a late customer of my bank who bears the same last name with you, {Peter Jongsman}, unfortunately he was among the death casualties in the May 26 2006 Earthquake disaster in Jawa, Indonesia that killed over 5,000 people. He was in Indonesia on a business trip and that was how he met his end. He was really close to me because I was his Account officer and manage his account. Do you in anyway related to him? May his soul rest in peace. So when I saw your last name, I was eager to read about you.

I can give you some hints about my country. United Arab Emirates is a beautiful country in the Middle East, that neighbor's with Saudi Arabia to the west and south, Qatar to the north, and Oman to the east. Most of the land is barren and sandy. U. A. E about 2.6 million. U. A. E became a federation in 1971 by seven Emirates known as the Trucial States, Abu Dhabi (the largest), Dubai, Sharjah, Ajman, Fujairah, Ras al-Khaimah, and Umm al-Qaiwain. In addition to a Federal President and Prime Minister, each Emirate has a separate ruler who oversees the Local Governing.

Our currency is called Dirham and exchange to US dollar 3.666 to $1. U. A. E has Crude Oil as major natural resources, and source of income to the Government. Tourism also yields money to the U. A. E Government. This is a little about my country and I hope you didn't get bored reading through the lines of my message. It gives me pleasure explaining the above to you and I will be waiting for your communication in regards to the information I asked for above.

Have a nice day and I do expect your communication. I am on skype online with this ID "abdullaqassem" and send me your personal email as while. Mine is abdullaqssem04@yahoo.co.in.

Figure 5 - Second contact

A fairly rapid response is provided (Figure 5), and things start to get more interesting. Continued difficulty with English expression and grammar reinforces the idea that the user does not have English as their first language (some observers might suggest that it reflects a person thinking in the structure of their primary language and then translating as they speak / write). The rapid change of subject matter and message content is a warning sign, suggesting an individual who is trying to rapidly establish a rapport and level of trust before making a move that otherwise would be caught out.

The user is passing themselves off as a moderate Muslim with grand plans for addressing issues they identify as being driven by radicalism. Combined with detailed data on the UAE, its currency, and information about current weather conditions, as well as requests about Australian IT and VC sectors, the user has gone to a lot of effort to appear as the real Abdulla Qassem (or has reasonable Google-Fu and Wiki-Fu).

This fails to hide three major warning signals. The first is the apparent bait for the phish / scam (the death of a customer in Indonesia), second is the provision of a Skype account when the UAE is known to actively block Skype, and the third is the still-incorrect email address (which has

been checked by this time), with the same spelling mistake. This message also starts to see the repeat of requests for information freely available from Carl's Ecademy account, as well as the incorrect repeating of simple data (such as Carl's name) - yet another warning sign.

A successful test to the correct Yahoo! email account generated the first of several emails to Sûnnet Beskerming (Figure 6).

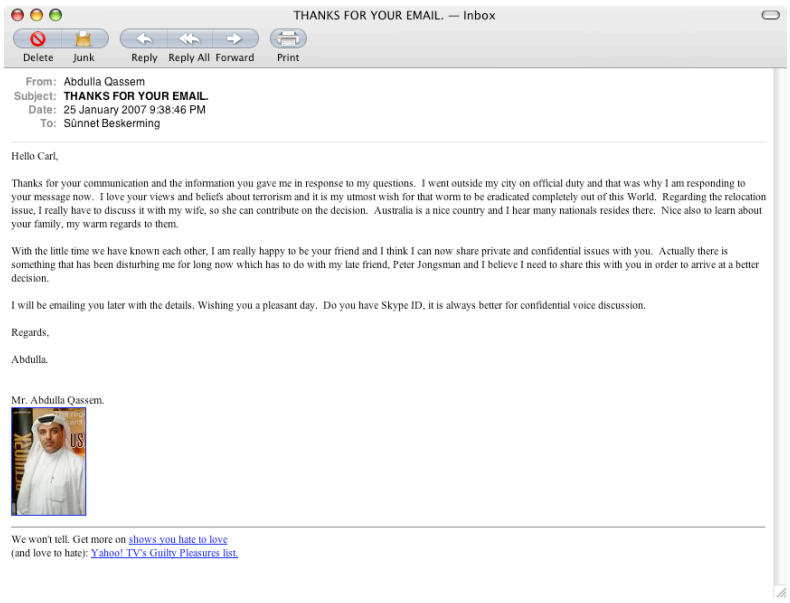


Figure 6 - The first email received

Now that we are no longer constrained by the Ecademy site, and we have shown a willingness to keep talking, Abdulla Qassem now starts to throw out more of the bait, promising confidential information to be passed in due course.

By this stage, most recipients should be able to identify this as an early stage phishing / scamming attempt. The problem is that the user has built up a rapport by this stage, to the point that a fair level of trust is established. Mixing the phish in with legitimate conversation is designed to overcome the recipient's natural reaction to identify it as a malicious message.

Finding a Clone

Because of the contradictory signals being given by the email, a check of the source code behind the message (there should be nothing to worry about there, right?) and a look at the headers to see where it has come from should drive the results one way or the other. All emails showed the same footer code (including the image), and also the same original source IP. This pattern is not normally a problem when dealing with the same individual, except this time it provided the evidence to verify that the Abdulla Qassem we were talking with was not the real one.

```
opportunity.<BR><BR>Regards,<BR><BR>Carl<BR></BLOCKQUOTE><BR><BR><BR><DIV>Mr. Abdulla Qassem. <BR></DIV>  <DIV><A href="http://
images.google.com/imgres?imgurl=http://www.ameinfo.com/images/news/4/17794-abdull.jpg&amp;imgrefurl=http://www.ameinfo.com/news/
Company_News/N/Network_International/&amp;h=320&amp;w=220&amp;sz=17&amp;hl=en&amp;start=8&amp;tbnid=zCeD-
Csdq7DMUM:&amp;tbnh=118&amp;tbnw=81&amp;prev=/images%3Fq%3Dabdulla%2Bqassem%26svnum%3D10%26hl%3Den%26lr%3D%26sa%3DN"><IMG style="BORDER-
RIGHT: 1px solid; BORDER-TOP: 1px solid; BORDER-LEFT: 1px solid; BORDER-BOTTOM: 1px solid" height=118
 src="http://images.google.com/images?q=tbn:zCeD-Csdq7DMUM:http://www.ameinfo.com/images/news/4/17794-abdull.jpg" width=81></A></
DIV><p>&#32;
```

Figure 7 - The code behind the image

The HTML code (Figure 7) that generates the image and link at the base of the emails from Abdulla Qassem is actually a Google Image Search (Figure 8), linking directly to the first image from the search - specifically to Google's thumbnail.

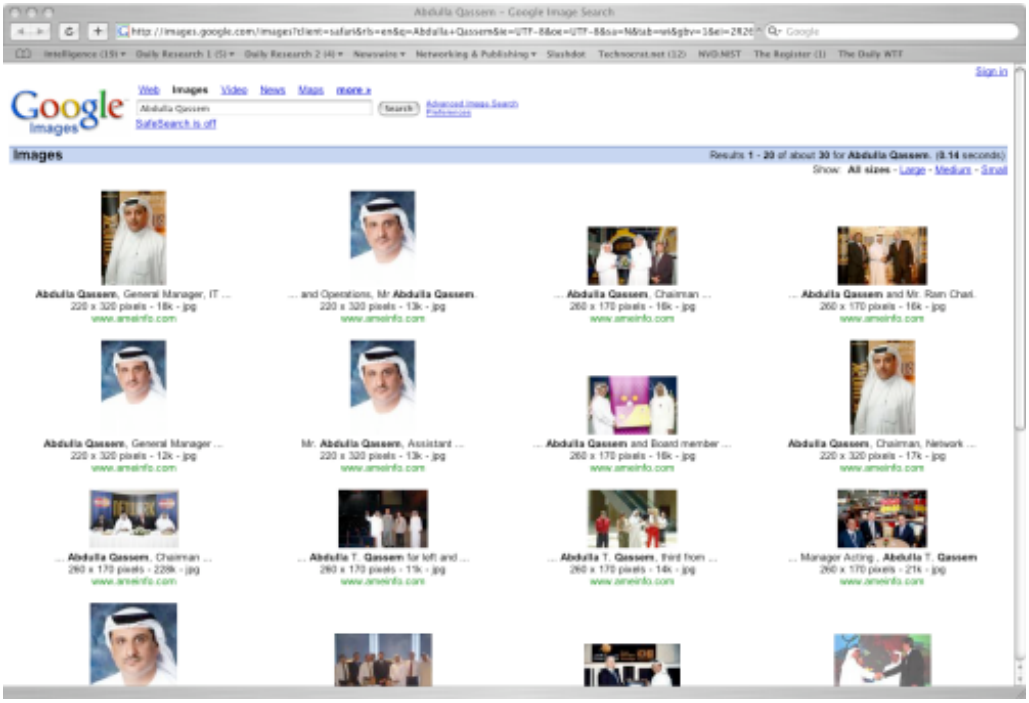


Figure 8 - Google Image Search, used to insert email images

This alone is not enough to confirm that we are not talking with the real Abdulla Qassem, it could just be that he chooses to rely on Google for image support, rather than hosting the image himself, or attaching it to the email.

```
Received: from [193.220.212.22] by web58903.mail.re1.yahoo.com via HTTP; Fri, 26 Jan 2007 01:33:11 PST
Date: Fri, 26 Jan 2007 01:33:11 -0800 (PST)
```

Figure 9 - We know where you are - Email header

The real evidence comes from the email header on each message received from Abdulla. Every message passes through the Yahoo! mail system to the Sûnnet Beskerming account from the abdullaqassem04@yahoo.co.in / abdullaqassem04@yahoo.com addresses, and all originate from the IP address 193.220.212.22 (Figure 9).

Running a 'dig' on this address returns

```
220.193.in-addr.arpa.    10800  IN SOA      parabol.taide.net. hostmaster.taide.net.
```

This information is interesting as taide.net supply coverage to Africa and the Middle East, so it is possible that our Abdulla Qassem is in the Middle East.

Armed with this information, we perform a 'whois', using whois.ripe.net, which returns

```
% Information related to '193.220.212.0 - 193.220.214.15'
inetnum:       193.220.212.0 - 193.220.214.15
netname:       RAINBOW-LTD-ENUGU-NG
descr:         Rainbow Limited
country:       NG
admin-c:       RADM3-RIPE
tech-c:        RADM3-RIPE
status:        ASSIGNED PA
remarks:       ----------
remarks:       T-IP-20040803
remarks:       ----------
mnt-by:        TAIDE-NOC
mnt-lower:     TAIDE-NOC
source:        RIPE # Filtered

person:        Rainbownet Network administrator
address:       Rainbownet Limited, Plot 3 Ebeano Estate
address:       Enugu, Nigeria
phone:         +234 42 306392
fax-no:        +234 42 306393
e-mail:        admin@rbow.net
nic-hdl:       RADM3-RIPE
source:  RIPE # Filtered
```

Now, we have some really useful information. From this, we know that 'Abdulla Qassem' is currently in Nigeria, connecting through Rainbownet - which proudly serves South-East Nigeria and not the UAE.

Using this data, we are able to have Ecademy suspend the account of Abdulla Qassem, while we begin trying to talk to him via Skype Instant Messaging (Figure 10).

Figure 10 - Not the real Abdulla Qassem (Skype User Profile)

Even though we know that we are not talking to the real Abdulla, we want to see exactly what he had in plan. The trimmed (quiet periods and irrelevant content removed) Skype log is attached following the Glossary.

Key events to look for are when he claims he has been busy on the phone - in reality he has been busy trying to recreate his Ecademy account as the Ecademy staff and I quickly shut down each account he creates (Figure 11). Also, he claims to have an appointment he needs to keep. This only comes up once we declare that he is a fraud. Once direct questions about banking procedure and other processes he doesn't want to answer are asked he ducks and weaves from the answers or just ignores them.

Figure 11 - The Ecademy account as it is now

Current Situation

During the creation of this report, the originating IP for the attacks was taken offline - which was confirmed via traceroute and ping. It is possible that one of the third party agencies that the incident has been reported to was able to convince the ISP to disconnect the offending system, but it is just as likely that the phisher has been spooked and has decided to take their system offline. At the same time, the fake Abdulla Qassem has not reappeared on Ecademy or on the Skype network.

As it stands, this new style of phishing and scamming is more like an old style scam, from when there was no Internet, and con artists had to invest time and resources into making a successful scam. Without getting the answer from the fake Abdulla, it is difficult to say what sort of return for his time he was getting, but given that he was targeting business operators and users, he was tapping into a potentially very large source of funds.

5. What Can Be Done?

As with almost every other Information Security issue, improving the overall situation requires contribution from at least two parties - the end users, and the service providers.

End Users

Put simply, what end users need is education. By reading through this document, it will go along way to educating end users about the risks they face when going online and interacting with the various networking sites that they might be a part of.

Service Providers

By now, most email providers and ISPs should have robust procedures and practices in place to ensure that complaints and reports of abuse are quickly addressed and acted upon. Unfortunately, too many service providers still ignore third party reporting and notification, and that includes some of the largest service providers.

Networking site operators have traditionally had less exposure to the malicious phishing, spamming and identity fraud that has normally been perpetrated via email and other malware, but it has become a real problem for them in recent years. If they haven't done so already, site operators need to ensure that their users can rapidly notify them of any problems that they have encountered (or believe they have encountered) with the site or other users on the site. Whether this is a link on each account page inviting the viewer to 'Complain', such as Ecademy uses (Fig-

ure 12), or it requires the user to navigate to Customer Service and lodge their issues, it needs to be readily available to the average user, and simple enough for them to rapidly find it and lodge an issue.

Figure 12 - The all important Ecademy Setting

Once an issue has been lodged, site operators need to be timely in how they deal with the concerns. In some cases it will be a matter of seconds or minutes (as Ecademy were able to respond and suspend the fake accounts once notified), but in all cases it needs to be as quick as possible in order to minimise the ongoing risk to other site users. Most importantly, site operators need to acknowledge to the concerned user that the issue has been received and is being acted on.

Unfortunately, this style of fraud is extremely difficult to guard against, from the site operators' point of view, and it will always be a case of needing to be alert and responsive to notification. If site operators can provide users with a list of signs to be cautious of, it will go a long way to fixing the situation.

6. About Sûnnet Beskerming

Sûnnet Beskerming is an Information Security company with a difference. Formed in early 2004 in Adelaide, Australia, Sûnnet Beskerming was created to develop and commercialise advanced Information Security research. Sûnnet Beskerming Pty. Ltd. is an Information Security specialist and, in conjunction with the tools developed in house, provides total security solutions and services, from the perimeter to internal data stores, including web application security and security testing and analysis.

Glossary

A) 419

When used in relation to phishing / scams it refers to the section of the Nigerian Criminal Code that is violated by Advance Fee Fraud, which is the most common form of scam associated with Nigeria-based scammers.

B) Google-Fu

A term which describes the ability to develop superior searches on Internet search engines, and so obtain better results and information faster than anyone else.

C) Phisher

The person (phishers when plural) who is busily engaged in a phishing attempt, or one who phishes.

D) Phishing

Derived quite poorly from 'Fishing', the term represents an Internet-based attacker leaving 'bait' for an unsuspecting user (such as an email message and compromised website) that entices them to voluntarily give up sensitive personal and financial information without being able to identify a breakdown of trust.

E) Ping

In the context of this report, ping refers to the command line tool that can be used to probe a remote networked system for a response. In addition to verifying the availability of a system on a given network address, ping provides guidance on the reliability of the network connection between the systems.

F) Professional / Business Networking Site

A site that is designed to allow users to establish business and personal network links with other users, with the goal of improving professional relationships and business opportunities. These sites can be considered the business equivalent of MySpace[4] and FaceBook[5]. Examples include Ecademy[6], LinkedIn[7], ...

G) Skype[8]

One of the many different Voice over IP (VoIP) applications available for users who wish to partake in Internet telephony. A number of countries and ISPs try and prevent their users from using this, and similar applications. One of these countries is the United Arab Emirates.

H) Sports Phishing

Yes, it is a term we made up (even though Deb Radcliff at Computerworld has been seen using it before us). No, we don't want to see it spread across the Internet. Our version of the phrase is meant to represent the sporting

[4] http://www.myspace.com

[5] http://www.facebook.com

[6] http://www.ecademy.com

[7] http://www.linkedin.com

[8] http://www.skype.com

challenge of getting the phisher to commit to the chase without the bait being taken.

I) Traceroute

A command line tool that is used to identify the route that network traffic is taking between two endpoints. It is a useful tool when investigating possible network difficulties.

J) Webmail

In the context of this report, Webmail refers to the various free online mail services offered by providers such as Yahoo!

K) Wiki-Fu

Similar to Google-Fu, except it relates to the ability of a researcher / Internet user to extract data from Wikipedia and other similar sources.

www.beskerming.com

Skype Log

Sunnet Beskerming:	19:36:40	Hello Abdulla, it's Carl from ecademy. How are you doing?
Abdulla Qassem:	19:37:04	how are you?
Abdulla Qassem:	19:37:07	good morning
Sunnet Beskerming:	19:37:08	I was recently on ecademy and I noticed that your account has been suspended. Is everything okay?
Abdulla Qassem:	19:37:29	I have been on guest user
Sunnet Beskerming:	19:37:53	I know, but it looks like the company has cancelled your account.
Abdulla Qassem:	19:38:11	no not cancelled
Abdulla Qassem:	19:38:43	I need to reload my card and pay for the service
Sunnet Beskerming:	19:38:46	?
Sunnet Beskerming:	19:38:52	What card?
Abdulla Qassem:	19:38:59	credit card
Sunnet Beskerming:	19:39:07	Okay.
Abdulla Qassem:	19:39:20	so how are you today?
Sunnet Beskerming:	19:39:29	I am doing quite well, yourself?
Sunnet Beskerming:	19:39:52	You were going to ask me something about your client who passed away, what was it?
Abdulla Qassem:	19:39:52	I am ok
Abdulla Qassem:	19:40:09	today is a work free day here in UAE
Sunnet Beskerming:	19:40:19	Okay
Abdulla Qassem:	19:40:26	so I am at home
Abdulla Qassem:	19:40:52	I have your email and will be emailing you details
Abdulla Qassem:	19:41:17	though we can discuss it now, are you in a secure place now?
Sunnet Beskerming:	19:41:22	Yes, are you?
Abdulla Qassem:	19:41:46	yes

Sunnet Beskerming:	19:41:56	Okay, I'm ready
Abdulla Qassem:	19:42:23	Peter Jongsman
Abdulla Qassem:	19:42:39	like I told you was a customer to my bank
Abdulla Qassem:	19:42:57	and I was the person that brought him into the bank
Sunnet Beskerming:	19:43:00	Yes, who died in the Indonesian earthquake. What city was he in?
Abdulla Qassem:	19:43:06	yes
Abdulla Qassem:	19:43:25	I knew him way back in the University in America
Abdulla Qassem:	19:43:48	so when I got the bank wok and he was also into Crude Oil deals
Abdulla Qassem:	19:44:08	and shuttles all the Middles East countries
Abdulla Qassem:	19:44:22	so I brought him to bank with us
Abdulla Qassem:	19:44:56	the issue is that he left some money in my bank,
Abdulla Qassem:	19:45:11	a huge amount
Abdulla Qassem:	19:45:32	he was not married and had no child
Abdulla Qassem:	19:46:04	I have tried to locate any of his likely relatives since his death, but to no avail
Abdulla Qassem:	19:46:26	that was why when I saw your last name I got interested to know you more
Abdulla Qassem:	19:47:08	you there?
Sunnet Beskerming:	19:47:35	Yes. I am just curious as to how you have managed to get Skype working around Etisalat's restrictions.
Abdulla Qassem:	19:48:21	I am into IT, so break through their Network
Abdulla Qassem:	19:48:50	you know Etisalat?
Sunnet Beskerming:	19:49:20	I just know that they block Skype.
Sunnet Beskerming:	19:49:23	How did you do it?
Sunnet Beskerming:	19:49:33	I guess Etisalat is your ISP?
Sunnet Beskerming:	19:51:17	Hello?

Sunnet Beskerming:	19:52:12	If you are still there, I am interested in finding out more about my distant relative (I assume we are related somewhere in the past). What degree did he do at University?
Abdulla Qassem:	19:52:48	sorry I was on the phone
Sunnet Beskerming:	19:53:04	Can you answer my questions from above?
Abdulla Qassem:	19:53:23	I am using service through my bank's network and not most of the sites are blocked
Abdulla Qassem:	19:54:42	we make use of Skype from the bank's network
Sunnet Beskerming:	19:55:28	Okay.
Sunnet Beskerming:	19:55:42	What did my relative do at University?
Abdulla Qassem:	19:56:03	he studied business administration
Sunnet Beskerming:	19:56:05	I see you are back on Ecademy
Sunnet Beskerming:	19:56:17	?
Abdulla Qassem:	19:56:33	yes l just signed in as guest member
Abdulla Qassem:	19:56:47	but will last for 14 days
Sunnet Beskerming:	19:57:01	Okay
Sunnet Beskerming:	19:57:52	You were saying that my relative had left his account with you?
Abdulla Qassem:	19:58:18	pls still on the phone, will get back immediately
Sunnet Beskerming:	19:59:04	What happened? Your Ecademy account vanished again?
Sunnet Beskerming:	19:59:33	I can't see it any more, is everything okay?
Abdulla Qassem:	19:59:58	l can't really say
Abdulla Qassem:	20:00:19	what is the problem
Sunnet Beskerming:	20:00:56	Okay. Can you please send a short test email to me. I need to check that I copied down the correct email address.
Abdulla Qassem:	20:01:31	l just received your email
Sunnet Beskerming:	20:02:01	Yes. I had three different addresses. Can you please send a quick reply so that I know which one to use.
Abdulla Qassem:	20:02:27	ok

Abdulla Qassem:	20:02:37	will do that immediately
Abdulla Qassem:	20:03:35	check your email now
Sunnet Beskerming:	20:04:30	Thank you. I've got it.
Sunnet Beskerming:	20:04:58	Tell me more about the problem that my relative has left you with.
Abdulla Qassem:	20:05:20	ok will explain in details now
Abdulla Qassem:	20:06:51	l will be with you now
Sunnet Beskerming:	20:07:15	Okay
Abdulla Qassem:	20:08:38	let l was saying, Peter Longsman left some money before he died
Sunnet Beskerming:	20:09:57	Yes
Abdulla Qassem:	20:10:44	now there is a new development here concerning finance and if nothing is done, the funds will be confiscated
Abdulla Qassem:	20:11:23	I have searched everywhere for any close relative of him, but did not succeeded
Sunnet Beskerming:	20:12:51	okay
Abdulla Qassem:	20:13:24	so l need suggestion on what to about the issue now
Abdulla Qassem:	20:13:52	my bank management is yet to know that Peter is death
Sunnet Beskerming:	20:15:07	?
Abdulla Qassem:	20:15:47	I am ye to inform them about this, because they will request for his inheritor
Abdulla Qassem:	20:16:03	whhich I cannot provide now
Sunnet Beskerming:	20:16:21	Did you try the University Alumni Association?
Abdulla Qassem:	20:16:25	I want to conclude on a decision before breaking the news to them
Sunnet Beskerming:	20:16:45	So, what are you considering?
Abdulla Qassem:	20:17:00	I have, but no one has any clue about him
Abdulla Qassem:	20:17:32	I am sure he died in that quake, because I spoke with him minutes before it happened
Sunnet Beskerming:	20:18:38	What are the options you are thinking of?

Abdulla Qassem:	20:19:21	I have been thinking of this
Abdulla Qassem:	20:19:57	the only option is to find someone to present as his hier
Sunnet Beskerming:	20:20:15	Is that legal?
Sunnet Beskerming:	20:22:14	Hello?
Abdulla Qassem:	20:22:52	yes, the way I plan it, it will be legal
Sunnet Beskerming:	20:23:08	What is the way you have planned it?
Sunnet Beskerming:	20:23:17	And, how much money are we talking about?
Abdulla Qassem:	20:24:41	in his checking account, there is nothing much there
Abdulla Qassem:	20:24:55	about $3,000
Abdulla Qassem:	20:25:39	but in the fixed deposit account, he has $18.7 million
Abdulla Qassem:	20:25:49	in American dollars
Sunnet Beskerming:	20:25:51	So, what is your plan?
Abdulla Qassem:	20:27:02	my plan is to get someone to present as his next of kin, with my position in the bank I will input the person's details in the Peter's file in bank system
Sunnet Beskerming:	20:27:16	and?
Abdulla Qassem:	20:27:27	I am incharge of my bank's IT, so I can manipulate that
Abdulla Qassem:	20:28:01	once this is done, I will then notice the management that Peter is late and his hier wishes to apply for the release of the account
Abdulla Qassem:	20:28:25	I am Peter's account officer and should have information about him
Sunnet Beskerming:	20:28:32	And then?
Abdulla Qassem:	20:28:34	that is the system
Abdulla Qassem:	20:28:58	then the person will apply for the claim through an attorney here in UAE
Abdulla Qassem:	20:29:18	and I will assist to facilitate other things in the bank
Sunnet Beskerming:	20:29:56	That's very nice of you. The bank must be paying you well to do this for their clients.

Abdulla Qassem:	20:30:38	you don't understand, if I do not do it, the bank management will do
Abdulla Qassem:	20:30:48	they will take the funds for their personal use
Sunnet Beskerming:	20:31:20	I understand. The bank must be paying you well for you to go to so much effort for their clients.
Abdulla Qassem:	20:31:41	I don't get you here?
Sunnet Beskerming:	20:33:20	I haven't seen any bank account managers who have gone so far out of their way for a client before. You must be really special.
Sunnet Beskerming:	20:33:37	Surely you aren't doing all of this work for free?
Abdulla Qassem:	20:34:20	Peter was a classmate and when he needs a bank in Middle East he talked to me, is there anything wrong about it?
Sunnet Beskerming:	20:35:15	Are there any fees involved with getting the money out?
Abdulla Qassem:	20:35:39	I do not understand,
Abdulla Qassem:	20:35:46	clarify pls
Sunnet Beskerming:	20:36:38	What fees are involved with extracting the $3000 and the $18 .7 million?
Abdulla Qassem:	20:37:14	you mean the legal aspect of it?
Sunnet Beskerming:	20:37:28	Any part of it?
Abdulla Qassem:	20:37:34	if that is what you mean, I will handle that aspect
Sunnet Beskerming:	20:37:45	What happens now?
Abdulla Qassem:	20:38:30	what happens is to know if you will be interested to assist me, if yes then we discuss terms
Sunnet Beskerming:	20:38:45	What terms?
Abdulla Qassem:	20:39:27	terms on the $18.7
Sunnet Beskerming:	20:39:35	What are they?
Abdulla Qassem:	20:39:59	you will state how you wish us to share it
Sunnet Beskerming:	20:41:13	Single lump sum only.
Abdulla Qassem:	20:41:33	pardon
Sunnet Beskerming:	20:42:09	Don't worry.

Sunnet Beskerming:	20:42:21	Assume that is done, what would need to happen next?
Abdulla Qassem:	20:43:06	are meaning to say when the claim is doen, what will happen? is that what you mean?
Sunnet Beskerming:	20:43:54	After terms are agreed to, what is the next stage?
Abdulla Qassem:	20:44:35	the next stage is to proceed with the process
Sunnet Beskerming:	20:44:45	Which is?
Abdulla Qassem:	20:45:52	I will require your address and phone numbers
Abdulla Qassem:	20:45:57	I have your full names
Sunnet Beskerming:	20:46:17	Is there anything else you need in addition to that?
Abdulla Qassem:	20:46:21	they are the information I need to input in the system
Abdulla Qassem:	20:46:27	no
Abdulla Qassem:	20:46:32	age
Abdulla Qassem:	20:46:39	and occupation,
Sunnet Beskerming:	20:47:34	Sounds fair enough. How will you know where to put the money?
Abdulla Qassem:	20:47:57	I don't understand
Sunnet Beskerming:	20:48:23	Once the money is released, how will you know where to put it?
Abdulla Qassem:	20:48:46	the bank will request account details from you for transfer
Sunnet Beskerming:	20:49:32	How soon can you start the process?
Abdulla Qassem:	20:50:05	the first issue to take care of is the changes
Abdulla Qassem:	20:50:16	once that is done, we commence
Sunnet Beskerming:	20:50:30	Yes. How quickly can that take place? Today? Tomorrow? Now?
Abdulla Qassem:	20:51:10	today is out of it
Abdulla Qassem:	20:51:28	if I have the details, I can do the changes before Monday
Sunnet Beskerming:	20:55:52	What happened to all the people you had contacted with your original Ecademy account? I know a number of them, would you like me to contact them and tell them what happened?

Abdulla Qassem:	20:56:41	no problem I will sort out the account problem
Sunnet Beskerming:	20:57:32	I don't think some of them will be very understanding.
Sunnet Beskerming:	20:57:45	Abdulla, another question.
Sunnet Beskerming:	20:58:55	Why is it that your name and details show up in a spam archive, with you pretending to have $17.5 million from the crash of AA Flight 587?
Sunnet Beskerming:	20:59:15	The email address is different, but it claims that it is you.
Abdulla Qassem:	20:59:46	where did you read that pls?
Sunnet Beskerming:	21:01:33	I found it while digging around for some information relating to something else. I saw your name and was very surprised. Was that you? I know that sometimes legitimate email is classified as spam, that could have been it.
Abdulla Qassem:	21:02:12	It can't be me of course
Sunnet Beskerming:	21:02:30	Okay.
Abdulla Qassem:	21:02:48	this is my first time of hearing such
Abdulla Qassem:	21:05:44	I have an appointment to keep
Sunnet Beskerming:	21:06:35	Can I keep you for a couple more minutes, please? I have something I really want to share with you.
Abdulla Qassem:	21:06:58	ok
Sunnet Beskerming:	21:07:30	I just need to ask one technical question. Do you know how webmail works?
Abdulla Qassem:	21:07:55	why do you ask?
Sunnet Beskerming:	21:08:06	Because I do.
Sunnet Beskerming:	21:08:15	You might be surprised at exactly what I know.
Abdulla Qassem:	21:08:54	ok that is fine
Sunnet Beskerming:	21:09:38	I know you are not from the UAE. I know that you are not Abdulla Qassem from the Emirates Bank. I know that you are from Nigeria. I know where you are. I know that Ecademy has been quickly racing to shut down your account. I know that you have been running a variation of this scam since late 2006.

Sunnet Beskerming:	21:10:11	What sort of payout have you been making from so much effort in phishing? Surely mass spamming gives a better return?
Abdulla Qassem:	21:10:13	how do you mean?
Sunnet Beskerming:	21:10:41	You are not from the Emirates.
Sunnet Beskerming:	21:10:57	You are not a mid-level executive with Emirates Bank
Abdulla Qassem:	21:10:59	how can you say that?
Sunnet Beskerming:	21:11:09	Do you know what I do?
Sunnet Beskerming:	21:11:20	Did you even bother to read my account profile when you first contacted me?
Abdulla Qassem:	21:11:42	I read and you are into networking
Sunnet Beskerming:	21:12:00	What sort of networking?
Abdulla Qassem:	21:12:03	does that give you the right to say who I am and who I am not?
Abdulla Qassem:	21:12:11	internet
Sunnet Beskerming:	21:12:59	Do you want me to tell you the mailing address of your ISP?
Abdulla Qassem:	21:13:30	I can as well tell yours?
Sunnet Beskerming:	21:13:38	You first.
Sunnet Beskerming:	21:14:55	I'm waiting.
Abdulla Qassem:	21:15:54	ok
Abdulla Qassem:	21:17:01	66.45.244.66
Abdulla Qassem:	21:17:26	that is your ip
Sunnet Beskerming:	21:17:30	No
Sunnet Beskerming:	21:17:32	Nice try
Abdulla Qassem:	21:21:24	I go now to keep my appointment
Abdulla Qassem:	21:21:31	will touch base soon
Sunnet Beskerming:	21:23:33	I'll humour you. What is the technique you are using to bypass the UAE's filter against Skype?
Abdulla Qassem:	21:24:16	if you want to learn, come straight and I will teach

Sunnet Beskerming:	21:24:52	Name one of the tools that you should be using, and / or one of the versions of Skype that has been able to defeat the filters.
Sunnet Beskerming:	21:28:56	Let me give you some friendly advice. Give up on the advance fee fraud scam.