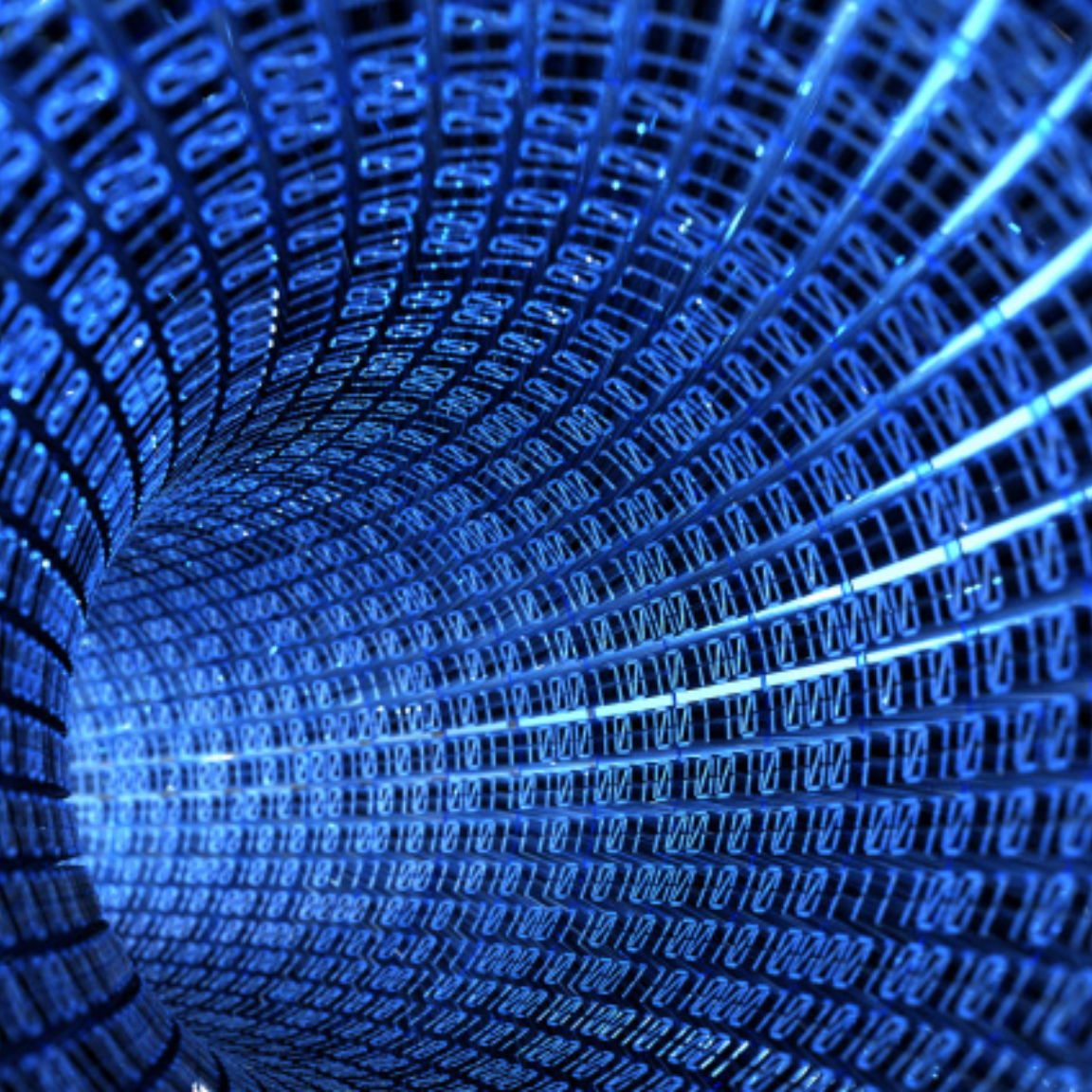
digitalcitizens alliance

DIGITAL CITIZENS ALLIANCE REPORT

GARTH BRUEN: THE FAKE CONFERENCE REPORT AND INTERNET PHISHING

TABLE OF CONTENTS



THE PHISH

Welcome to the Internet, where you may already a victim. Although this may be the case, it does not have to be. This story is about someone who chose not to be a victim, decided to take action, and what happened to her after the fact. This is also a story about correcting failure and what to do when you are confronted with a scam as well as what to do when the system fails. The power is in your hands to make a difference; you can demand a better Internet.

Phishing is a very serious cybercrime issue that targets millions of people and reaps large rewards for criminal organizations. A phishing email typically provides a link to a deceptive website. For example, recently I was contacted by a professional associate who received the following email:

Dear Colleague,

Its good to hear from you! Log on www.ccc12.org.uk to complete the registration and access fund application forms online respectively. Also send in your abstract or paper presentation at the earliest for appraisal and acceptance. See also the Frequently Asked Question section in our website: http://ccc12.org.uk/Faq.htm

We look forward to hearing from you at the earliest.

Regards!

Dr. Alex Cooke
Conference Chair

It may not immediately appear threatening, but the fact is that Dr. Alex Cooke does not exist and there is no conference call for papers. There are various sub-types of phishing out there, including fake professional conferences such as the one above. A fake professional conference is a scam in which the perpetrators attempt to get people to submit their personal information and make purchases for non-existent services. Shamefully, this particular conference targets many people in developing countries. Quickly, my associate suspected something was not right about this email. She knows a thing or two about how the Internet functions so she forwarded this phishing attempt to the service provider who sponsors the website. Most responsible service providers have abuse centers which process complaints about malicious websites, but in this case things got weird. The service provider, called a registrar, sloughed off the complaint to lower third party. Believe it or not, the third party told her it was not phishing. Shocked, she did her own follow up research and found scads of documentation proving that this was a fake conference scam. She forwarded this evidence back to the registrar who again rejected her complaint, basically telling her she did not know what she was talking about.

Then, she sent the whole thing to me, someone she knows works in this area. Regardless of all the frustrating condescension from the registrar, she did all the right things. We will explain in detail at the end how the registrar failed, but first let us review what went right. The potential victim used caution, good judgment; attempted to report the issue, validated the email, and asked a trusted person for advice. Only one aspect of this actually failed, but outside of the registrar all of her other instincts were rewarded.

The first step in protecting yourself from harmful Internet transactions is to consciously eliminate the idea that the virtual world is actually different or separate from the real world. Convenience blurs the thought of consequences, but if you pay a bill online do you not expect it to be paid in fact? Internet transactions are real, so when conducting Internet business, imagine physically handing your wallet or house keys to a stranger. Internet commerce is about speed, but just like going fast in a car, you need to be even more careful. There is an old saying in security: "trust but verify." I say, **just verify.** Trust in any relationship must be earned; it never comes first so if your gut tells you to be suspicious, listen to your gut.

WHAT SCAMMERS WANT FROM YOU

The Conference Chair, "Dr. Alex Cooke" in this case requests that you pay 300 British Pounds for registration and submit a research paper. It is bad enough to lose money to a scam, but I truly cringe at the thought of some poor researcher slaving to generate a document which will never be read, let alone published. Including the doctor title in the letter is a common trick to increase confidence in the reader. Research has shown that by simply wearing a white lab coat and introducing yourself as a doctor enhances trust even in the most ridiculous situations. [1]

It is important to understand the ultimate goal of any scammer in the broadest sense. The scammer's goal is a *transaction*. Transaction could mean an exchange of money, but for scammers it could also mean a victim surrenders personal information or access to secure accounts. Scammers do

not even need direct contact with a victim to obtain a transaction; sometimes it simply involves getting someone to believe something. The best example is in the phenomena of stock market spam. Pump-and-dump stock spam simply promotes a specific stock ticker code to artificially generate interest and push the price up. The sponsors of the spam campaign then sell their shares at the falsely inflated price, which then drops, leaving other investors with a loss.

Just like the stock scammers constantly change the target ticker, the imaginary conference group uses a number of ever-morphing names including:
The *Climate Change Impact Group, Climate Change Volunteer Conference*[2], *Global Warming Conference*[3] , *Global Warming Volunteer Group*[4] , and by the time you finish reading this article they will have invented a new one. In fact, the latest incarnation is called the *International Conference on Climate Change*[5] , at a site sponsored by the same registrar. However, it looks like "Dr. Alex Cooke" has retired and "Dr. Dale Martin[6]" is now the chair. Before "Dr. Martin" it was "Dr. Frank Bond[7]," "Dr. Murphy Burton[8]," and "Dr. Andrew Owen[9]."

---

[1] http://www.psychologytoday.com/articles/200203/the-man-who-shocked-the-world

[2] http://conference.researchbib.com/?action=viewEventDetails&eventid=20069&uid=r5bfd0

[3] http://www.419scam.org/emails/2012-01/23/00132091.1.htm

[4] http://www.ae-africa.com/read_article.php?NID=2673&tgt=post

[5] http://www.er.uqam.ca/nobel/spq/index.php/actualites/actualites-philosophiques/127-4th-international-conference-on-climate-change-london-9-13-november-2012-

[6] http://intccc.co.uk/media_partners.htm

[7] http://groups.yahoo.com/group/greatlakesrainbow/message/29345

[8] http://www.419scam.org/emails/2012-01/23/00132091.1.htm

[9] http://conference.researchbib.com/?action=viewEventDetails&eventid=20069&uid=r5bfd0

The website (now suspended, you can view the captured content here: ClimateChangeImpactGroupCCC2012Registration.pdf) is very convincing, mirroring many legitimate conference formats, and actually steals content from the real sites. This is not just an email problem. Trusted groups are unintentionally providing legitimacy to these fake conferences. Several versions of these fake conferences are listed in places like Research Bible[10] (researchbib.com) and the Societe De Philosophie Du Quebec[11] at the Universite du Quebec Montreal (er.uqam.ca/nobel/spq/) which simply list conferences of various types as a courtesy.

One might wonder reading this, *I'm not a climate scientist, why should I care?* The answer: because every profession is being targeted. I have spoken with lawyers, accountants, and bankers who have been touched by industry-specific phishing. Remember the issue in this scam is not even about climate science, it's about conferences. All trades have conferences. Scammers offer fake contracting services, building materials, furniture, car parts, everything. The scammers will attack one area over-and-over until "the well runs dry" and move on somewhere else. Your industry might be next. It is your duty to yourself and your community to take this seriously and share information.

Ask someone you trust already about suspicious emails, and don't be afraid to ask. I receive questions from other professionals regularly, really smart people in their own fields, who have questions about email. There is no shame in asking. The human impulse to not appear dumb in front of colleagues is something the scammers are counting on. They are hoping you are too proud to think you could ever be fooled and are too busy to check details.

---

[10] http://conference.researchbib.com/?action=viewEventDetails&eventid=20069&uid=r5bfd0

[11] http://www.er.uqam.ca/nobel/spq/index.php/actualites/actualites-philosophiques/127-4th-international-conference-on-climate-change-london-9-13-november-2012-

When verifying potential phishing emails do not use any of the contact details in the email or related websites. For example, if you receive a suspicious email from your bank, use the contact information for your local branch, information you already have. Our potential victim turned hero in this instance checked to see if the supposed climate science group was actually a registered organization in the United Kingdom at the Charity Commission (http://www.charitycommission.gov.uk/index.aspx). She also looked up supposed contact details for the conference which resulted in multiple reports of fraud.

Forward suspicious emails to known phishing working groups, there are several, listed below. These groups use the emails in their research and will take action if appropriate. Your data is *critical* to security researchers. They cannot do their work without real-world examples. If you assume "someone else" has already reported it, you might be wrong because someone has to be the first recipient. The scammers are counting on "smart" people to ignore phishing and not report it. Beyond being the first potential recipient, your email sample provides a unique perspective to a scam in its source or makeup which could be new details for an existing scam.

I speak at or attend at least ten conferences each year in my field. After doing this for a decade one might think I have heard of every group and meeting under the sun, but I am always finding new ones. It would not come as a surprise for a scientist to be invited to speak at a conference they previously knew nothing about. The fake conferences use the same language and imagery as the real ones, often stealing the actual content. So, before engaging in any transaction, ask a colleague in your industry. For example, there is a discussion group on LinkedIn called Environmental Experts where scientists have already started trading stories about these fake conferences[12]. Sadly, many postings are from people who have already been victimized.

[12] http://www.linkedin.com/groups/Warning-FRAUD-3212177.S.91283775

YOU CAN TAKE ACTION

It may surprise you, but there is an army of experts waiting to help with your phishing problem. If you received the phishing email at work, any in-house IT staff should be savvy enough to tell you if it is a scam email, report it for you, and possibly block it from your network. If the email came though on a public email service like Yahoo or Gmail, they also have built-in reporting services.

Computer security groups called "CERTs" (Computer Emergency Readiness Team) exist in many countries often sponsored by the government. US-CERT accepts phishing reports at phishing-report@us-cert.gov and provides detailed information on phishing at http://www.us-cert.gov/nav/report_phishing.html. Your tax dollars pay for this, use it.

One of the best resources available is the Anti-Phishing Working Group (APWG). The APWG conducts ongoing research into phishing and all types of cybercrime and sponsors regular conferences to analyze current threats. APWG accepts phishing reports at reportphishing@apwg.org and offer detailed information here: http://apwg.org/report-phishing/. APWG has also launched STOP THINK CONNECT (stopthinkconnect.org) which is great place for the ordinary Internet user to start protecting themselves.

If you want to research a possible phishing email, try Artists Against 419 (aa419.org). AA419 allows you to browse and search for phishing. Not sure your email is a phish? Look for it here: http://db.aa419.org/fakebankslist.php?ldsjkghm436.

Report it to Google: http://www.google.com/safebrowsing/report_phish/.
Staff at Google will investigate and they have the ability to block malicious sites from their searching and related browsers.

Tax season is fast approaching which means the fake IRS emails will be arriving soon. Unlike potential real emails from your bank, IRS emails do not exist. The top quote from the IRS phishing page is "The IRS does not initiate contact with taxpayers by email." There is no such thing as an email from the IRS. So, if you get one forward it to phishing@irs.gov or review more instructions here: http://www.irs.gov/uac/Report-Phishing.

WHAT TO DO IF YOUR A VICTIM

Report it to police and get your bank to cooperate. Government agencies have the tools needed to extract the hidden details of the scam. Your bank has transaction details which provide insight into the mechanics of the scam, this is critical to any investigation. It is not an easy task, but by peeling back the technical layers of a scam it is possible to find the criminals. If the Internet scam in particular involves a bank transaction (and they usually do) the FBI can investigate and you can get the ball rolling by filing a complaint with the IC3 (http://www.ic3.gov/), Internet Crime Complaint Center. This service is not for reporting phishing emails, but rather for reporting an actual transaction with a fraudulent party. The biggest obstacle in getting these crimes solved is the under-reporting by victims because they feel embarrassed. Don't. Everyone can be fooled; the worst thing you can do is to not report the crime and leave other unknowing individuals vulnerable.

IMPROVING INTERNET STANDARDS

Now we have to get into the gritty details of how the service provider failed, on several levels. If you had the power to stop a global scam targeting developing countries, would you? For most of us the answer is absolutely. Here, the registrar did the complete opposite for inexplicable reasons. In simple terms, the person running the fraudulent website is a customer of the registrar. The registrar has the duty to properly investigate abuse and the authority to terminate fraudulent websites. However, instead of handling the complaint, the registrar, eNom, referred the phishing email to subsidiary domain reseller called NameCheap. Resellers are agents of registrars. In turn, NameCheap rejected the complaint and informed the potential victim that it "cannot consider this case to be phishing-related." In making their bizarre determination NameCheap referenced the Wikipedia entry on Phishing. This is more shocking than simply ignoring the complaint as NameCheap is now engaging in the very dangerous behavior of reinforcing consumer misinformation by stating that this is not phishing. Instead of referring to the encyclopedia "anyone can edit" they should have read the very thorough BBC investigation from 2011 which had already labeled this specific scam as phishing[13].

However, here we specifically want to ask what the registrar should have done as a way of correcting this problem in the future? NameCheap clearly dropped the ball, but the truth is that they never should have been in charge of handling this abuse in the first place. Certainly, it is eNom's choice who they issue technical duties to,

[13] http://www.bbc.co.uk/news/science-environment-12219472

but NameCheap never should have been given the critical task of dealing with the victim. If eNom is trying to project a responsible front face for handling abuse they have completely ruined reputations by flushing this abuse report down to a reseller. By passing a serious issue to a third party eNom has lost control over its outcome, which in this case is disastrous. Not only did the third party fail to handle the complaint properly, they issued misinformation to a potential victim, reinforcing faith in a seriously malicious site. Registrars and other Internet service providers will often claim they have no power to stop crime on the Internet that is it beyond their scope and authority. However, eNom has stated policies concerning enforcement which do not match their behavior in this case:

"We have a zero tolerance spam policy.[14]."

At least what they present to the public sounds proactive, they also pledge that "eNom investigates and takes appropriate action with every Spam or security report that we receive.[15]" Of course there is the issue of whether or not eNom actually has the authority to act on complaints, but this is spelled out in the contract with their customers: "SERVICES PROVIDED AT WILL; TERMINATION OR SUSPENSION OF SERVICES…(ii) abuse of the Services…(iv) allegations of illegal conduct[16]" Then again, the bungling of this report was done at NameCheap, so what kind of standards does eNom demand from its resellers?

"You agree not to use the Services, or to allow Your customers or Sub-Resellers to use the Services for…Any illegal, dishonest, deceptive or unfair trade practices;[17]"

So, if eNom is not holding to its own agreement with NameCheap, is there anyone above eNom to hold eNom accountable? Yes, in this case because the scam site is a .UK domain it is handled by eNom under contract with the United Kingdom's sponsor Nominet (http://www.nominet.org.uk). Nominet grants registrars permission to sell .UK domains and license resellers but only under these conditions:

"we consider you to be responsible for the actions of your resellers, in other words the actions of your resellers are your responsibility[18]"

[14] http://www.enom.com/help/AbusePolicy.aspx

[15] http://www.enom.com/help/AbusePolicy.aspx

[16] http://www.enom.com/terms/agreement.aspx

[17] http://www.enom.com/terms/agreement.aspx?page=reseller

[18] http://www.nominet.org.uk/become-registrar/registrar-agreement/good-practice-terms

www.digitalcitizensalliance.org