SCAM – HOW IT WORKS…

Aug 17, 2017 | Security, Tips

"Hi. Just writing to let you know my trip to Manila, Philippines with my family has been a mess…I need you to loan me some money. I'll refund it to you as soon as I arrive home."

or…

"How are you and your family doing? hope this email find you all in good health and spirit. I am currently in Burkina

RECENT POSTS

An "Anti-virus update" e-mail could open you up to fraud

Oct 17, 2021 | CyberSecurity Month, Security

Tricks phishers use to hijack your university e-mail

Nov 22, 2019 | CyberSecurity Month, Security

Faso on vacation but i will return back as soon as possible due to my poor health. I have tried calling you severally but didn't get through, please can you call me on ... as soon as you get this email? I have something urgent i need to talk to you about."

That is the kind of fake e-mail thousands of university employees get every year. It appears to come from a friend or a colleague, but is actually from a scammer on the other side of the world.

All these scams have the same story, they were out of the country, they've been robbed and they need assistance now, or they are ill, or in some sort of trouble and need your help... This trick relies on good natured people willing to help a friend.

The Stranded Traveler scam is a way to profit from hacking into someone's webmail account – like Yahoo!Mail, Hotmail or GMail.

This usually happens when somebody has a simple, easily guessable password on their webmail account, or they have left their details on a phishing site.

Once the scammer has gained control of the "mule's" email account, they log into the webmail account and:

- Change the webmail password so the real user can't login.
- Grab a copy of all the contacts either from the contacts list or individual messages.
- Filter out non-personal messages to target friends/acquaintances only.
- Send the 'stranded traveler' message out to the contacts and hope for replies with money transfer details.
- Meantime the real owner of the webmail account is probably unaware there's a problem until they try

Phishing schemes that target academics

Oct 28, 2019 | CyberSecurity Month, Security

The threats of Malware and Ransomware: Part 2

Oct 7, 2019 | CyberSecurity Month, Security

The threats of Malware and Ransomware: Part 1

Oct 4, 2019 | CyberSecurity Month, Security

ARCHIVES

October 2021

to login to their email. Even then, they probably think they've forgotten the password rather than being hacked. It's only when a friend contacts them directly that the scam is revealed – usually far too late.

How to protect yourself: *There are various things you can do to prevent being a victim of this scam, either having your webmail hacked or receiving scam emails.*

- Don't click on attachments in emails from strangers, or if they are from someone you know but look suspicious.
- Have a complex, hard to guess password. Dictionary words aren't enough. Preferably a mix of upper and lower case letters plus digits and other characters like (!@#$%^&*)
- Don't reveal the password to anyone, and be careful of email messages that pretend to come from the webmail provider. Phishing messages are the most common way that people giveaway their passwords.
- If you get an urgent email from a friend, especially one asking for money, check with them using other means. Try to call them or check with mutual acquaintances to see if the story is true beyond what you've learnt in the email. At worst, you could reply and ask for some information only the real sender would know (keep in mind that the scammer can read/search the hacked webmail account).

So how do scammers get your email password?

- Phishing websites: Typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message are clicked onby the victim and they are directed to a malicious website set up to trick them into divulging personal information, such as usernames & passwords.

- Trojan programs: If you click on an attachment in an unknown email, it can trigger your computer to download a "Trojan" program that then allows cyber criminals to see every key stroke you make – including your email password.
- Password breaker program: Often called a "brute force program," this is software bad guys use to try every combination of numbers and letters until they hit on your password.
- Email addresses used as logons: You know how many websites have you set up an account using your email address as your User ID? If you then use the same password for that account that you use for email, criminals have what they need: your email address and your password.

SHARE:

‹ PREVIOUS

Spear-phishing is not a new water sport...

NEXT ›

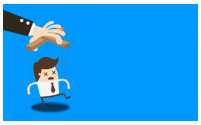
Phishing e-mails – a clear and present danger.

RELATED POSTS

Tricks phishers use to hijack your university e-mail

What is "Scareware"?

October 7, 2011



Cyber-Security Awareness Month – Social Engineering

A Guide to secure your Gmail Accounts against Gooligan

August 2013
July 2013
June 2013
April 2013
March 2013
May 2012
March 2012
November 2011
October 2011
June 2011
May 2011
April 2011
December 2010
October 2010
May 2010
April 2010
November 2009
October 2009
September 2009
August 2009

November 22, 2019

– The weakest link

October 24, 2018

December 7, 2016

July 2009

June 2009

May 2009

April 2009

March 2009