JCU SYSTEMS SECURITY CHAT

Why Are We Here Today?

There has been a noticeable increase in the number of online attacks targeted at JCU employees and students.

Objectives:

1. Discuss Basic Terminology
2. Provide guidance/advice regarding the use of reasonable security practices in the inter-connected world.
3. Communicate five take away items that you need to keep in mind.

STOP | THINK | CONNECT™

PII
Personally Identifiable Information

- PII – any data that could potentially identify a specific individual
  - name
  - SSN
  - passport number
  - driver's license number
  - credit card number
  - address
  - date/place of birth
  - mother's maiden name
  - medical, educational, financial, or employment information

FERPA

Family Educational Rights and Privacy Act

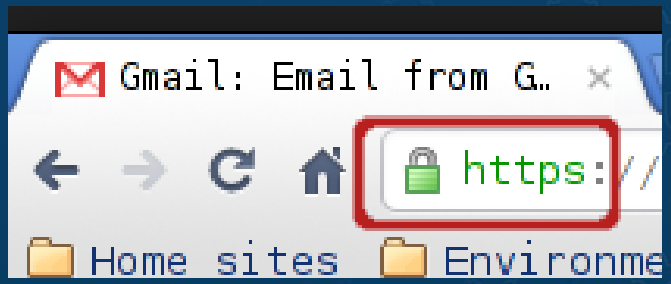
- Protects the privacy of student Education Records and sets requirements for release to 3rd parties.
- Education Records include any record directly related to a student and maintained by JCU or a JCU employee
  - transcripts
  - grades
  - classwork
  - papers
  - recommendations
  - housing information
  - conduct records
  - schedules
  - e-mail content
  - health information
  - contact / family information
- Office of Legal Affairs or the Registrar can assist

Use of PII / FERPA data

- Proper Use
  - *Minimum Necessary* basis
  - only available to authorized individuals
  - handled by 3rd parties as defined in a Business Associate Agreement, or as required by law
  - transmission & storage methods should be periodically reviewed with ITS & Legal Affairs
  - be especially cognizant of:
    - overheard conversations
    - faxes
    - copies / scans
    - printouts
    - email

Terminology

- Internet Browsing
  - http:// NOT Secure!
    - Data transmitted over the internet IS NOT encrypted. Use carefully!
  - https://



    - Certificates required for validation.
    - Use of **https://** is a **MUST** when any financial, personal, or private information is being transmitted online.
    - Information being transmitted IS encrypted from end point computer, tablet, phone to website computer on the other end.
  - Secure Wireless – eduroam
    - Ensures over-the-air encryption. Use network credentials. Allows "roaming" to participating institutions

Social Engineering
Phishing - Hacking – Malware - Spam

- **Social Engineering** - Social engineering is the art of manipulating /tricking people into breaking normal security procedures in order to have them divulge confidential information.
- **Phishing** - Using email, an instant message or text to masquerade as a trustworthy source (bank, company, government institution, school etc.) in an attempt to trick a user into surrendering sensitive information.
- **Hacking** - A hacker is someone who breaks into someone else's computer system, often on a network; bypasses passwords or licenses in computer programs; or in other ways intentionally breaches computer security.
- http://money.cnn.com/2017/09/11/pf/equifaxmyths/index.html
- **Malware** - Programs / apps that do bad things to your computer, phone, tablet etc.
- **Spam** - unsolicited, undesired, or illegal email messages.

Social Engineering Examples

- Fake Calls From:
  - Apple - Microsoft - Government Agencies IRS
    - They want to "Help" you: ($$$)
      - Pay an overdue bill, taxes, fines, lapsed memberships
      - Fix your computer, update its illegal operating system…….
  - JCU Examples:
    - "I received a phone call at home claiming to be from Microsoft's corporate headquarters about trouble with my computer."
    - Meritech p-card toner replacement
- Phony Password Reset Requests
  - The JCU Helpdesk requires last 4 SSN + Birthdate

Examples of Phishing at JCU

Hello,
This letter confirms a 3.84% increase on your monthly pay effective January 2015 paycheck.
Follow the link below to authenticate your credentials and read your pay increase letter.

CLICK HERE to access the documents

Sincerely,
Human Resources
John Carroll University

Phishing
"Account Activation" Scam

---------- Forwarded message ----------
From: **JCU ADMINISTRATOR** <knmejia@fucsalud.edu.co>
Date: Mon, Mar 2, 2015 at 4:34 PM
Subject: JCU EMAIL ACTIVATION 2015
To:

This mail is from your system admin help desk: It has come to our notice that there have been lot of spamming email receive from an unknown identify email senders
requesting you for your email information. To prevent email virus infection you are advised to Re-activate your email account access with the help line Re-activation link below, by clink on the link for reactivation.

Re-activation ---> click

A confirmation link will be send to you for the Re-Activation of your email after you have fill your datas on the admin link above Your confirmation is number: 1265-6778-8250. for a new activation.

Phishing
"CFO Wirefraud" Scam

From: Richard Mausser [mailto:rmausser@jcu.edu]
Sent: Wednesday, January 13, 2016 11:24 AM
To: twisz@jcu.edu
Subject: Urgent

Process a wire of $9,500.00 USD to the attached wiring instructions. This should be coded to Admin Expenses. Let me know when it is completed.

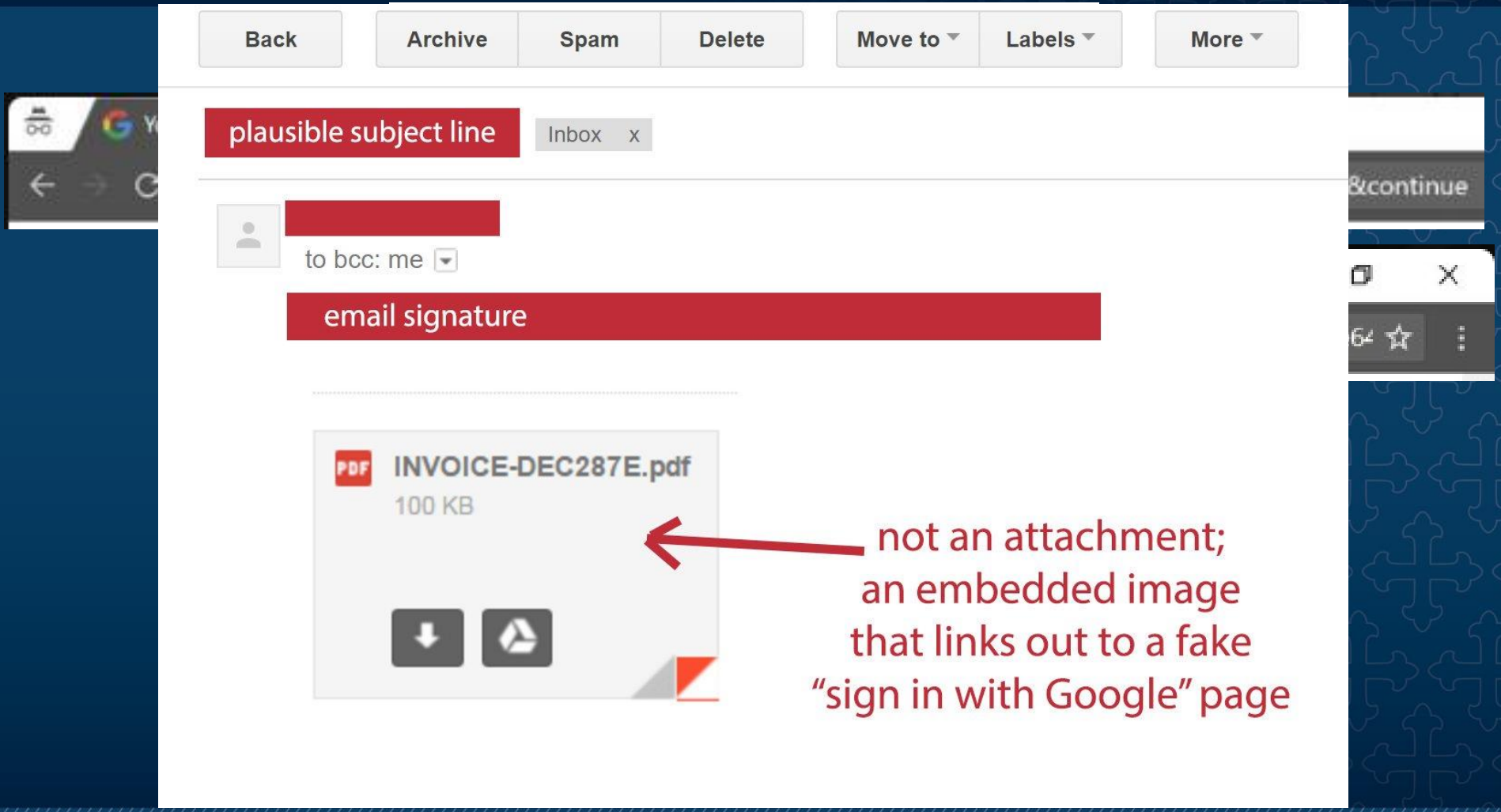
Thanks,
Richard

Phishing
"CFO Wirefraud" Scam

Delivered-To: twisz@jcu.edu
Received: by 10.112.6.170 with SMTP id c10csp3350849lba;
Wed, 13 Jan 2016 08:24:19 -0800 (PST)
X-Received: by 10.98.13.195 with SMTP id 64mr31903101pfn.164.1452702259489;
Wed, 13 Jan 2016 08:24:19 -0800 (PST)
Return-Path: <jchaffin@jcelectric-inc.com>
Received: from p3plwbeout01-04.prod.phx3.secureserver.net (p3plsmtp01-04-2.prod.phx3.secureserver.net. [72.167.218.88])
by mx.google.com with ESMTPS id x83si2931637pfi.25.2016.01.13.08.24.18
for <twisz@jcu.edu>
(version=TLS1_2 cipher=AES128-SHA bits=128/128);
Wed, 13 Jan 2016 08:24:19 -0800 (PST)
Received-SPF: neutral (google.com: 72.167.218.88 is neither permitted nor
guess record for domain of jchaffin@jcelectric-inc.com) client-ip=72.167.21
Authentication-Results: mx.google.com;
spf=neutral (google.com: 72.167.218.88 is neither permitted nor denied
record for domain of jchaffin@jcelectric-inc.com) smtp.mailfrom=jchaffin@

Received: from localhost ([72.167.218.4])
by p3plwbeout01-04.prod.phx3.secureserver.net with bizsmtp
id 5UQJ1s00106H1ow01UQJ0m; Wed, 13 Jan 2016 09:24:18 -0700
X-SID: 5UQJ1s00106H1ow01
Received: (qmail 15696 invoked by uid 99); 13 Jan 2016 16:24:18 -0000
Content-Type: multipart/mixed;
boundary="=_a997c568edfc4ed1ef274e9d80b0292e"
X-Originating-IP: 151.227.204.123
User-Agent: Workspace Webmail 5.16.0
Message-Id: <20160113092416.fd448a813869919af386f149432a30f7.3987de28e9.wbe@email01.secureserver.net>
From: "Richard Mausser" <rmausser@jcu.edu>
X-Sender: jchaffin@jcelectric-inc.com
Reply-To: "Richard Mausser" <finance-controller@outlook.com>
To: twisz@jcu.edu
Subject: Urgent
Date: Wed, 13 Jan 2016 09:24:16 -0700
Mime-Version: 1.0

Phishing
"Fake" Google



Malware "FedEx" distribution

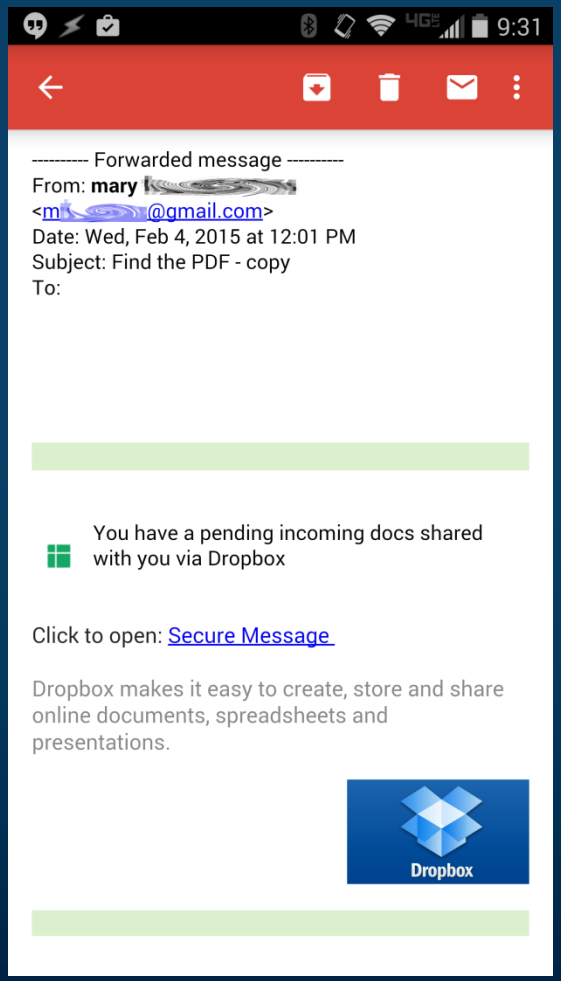
From: **FedEx International Next Flight** <phillip.odell@50-87-151-118.unifiedlayer.com>
Date: Thu, Mar 19, 2015 at 7:54 AM
Subject: We could not deliver your parcel, #0000936471
To: [redacted]@jcu.edu

Dear Customer,

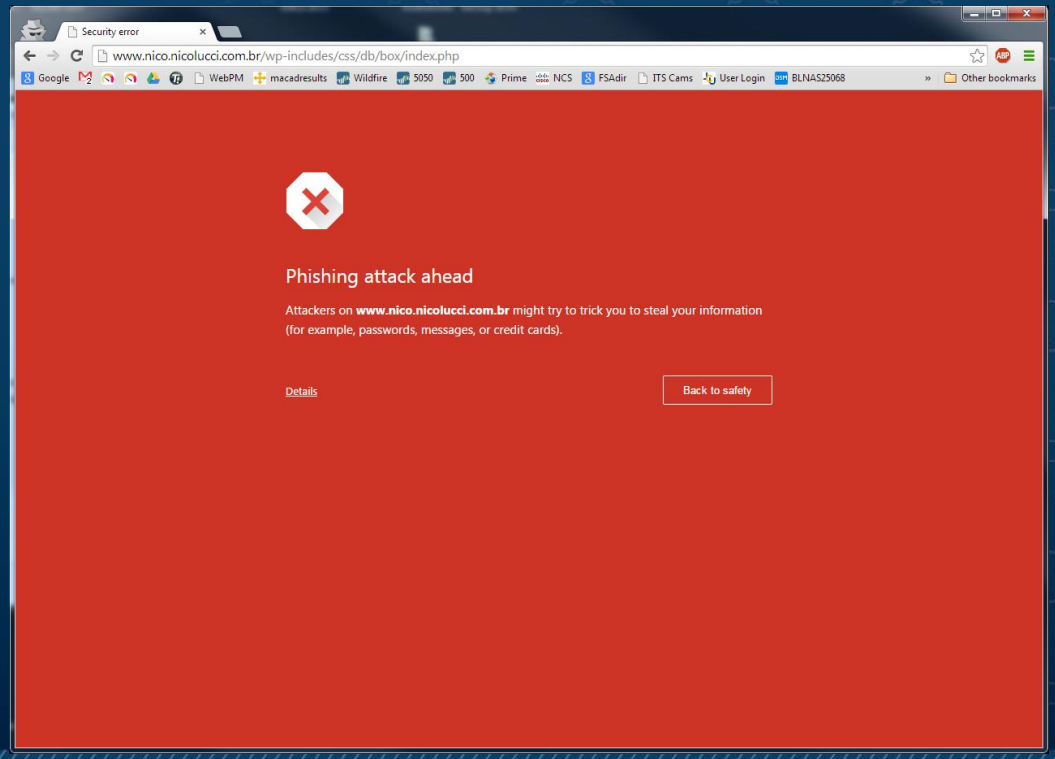
Courier was unable to deliver the parcel to you.
Delivery Label is attached to this email.

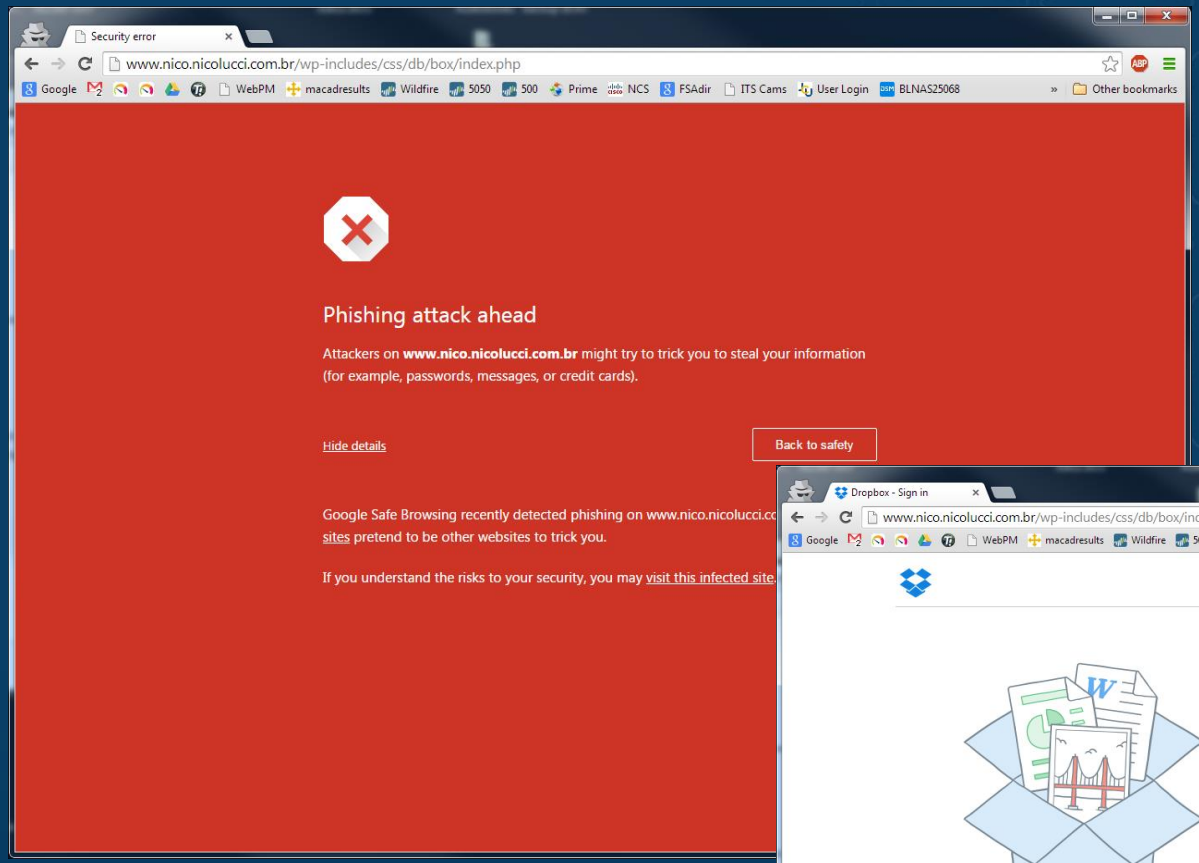
Warm regards,
Phillip Odell,
FedEx Station Agent.

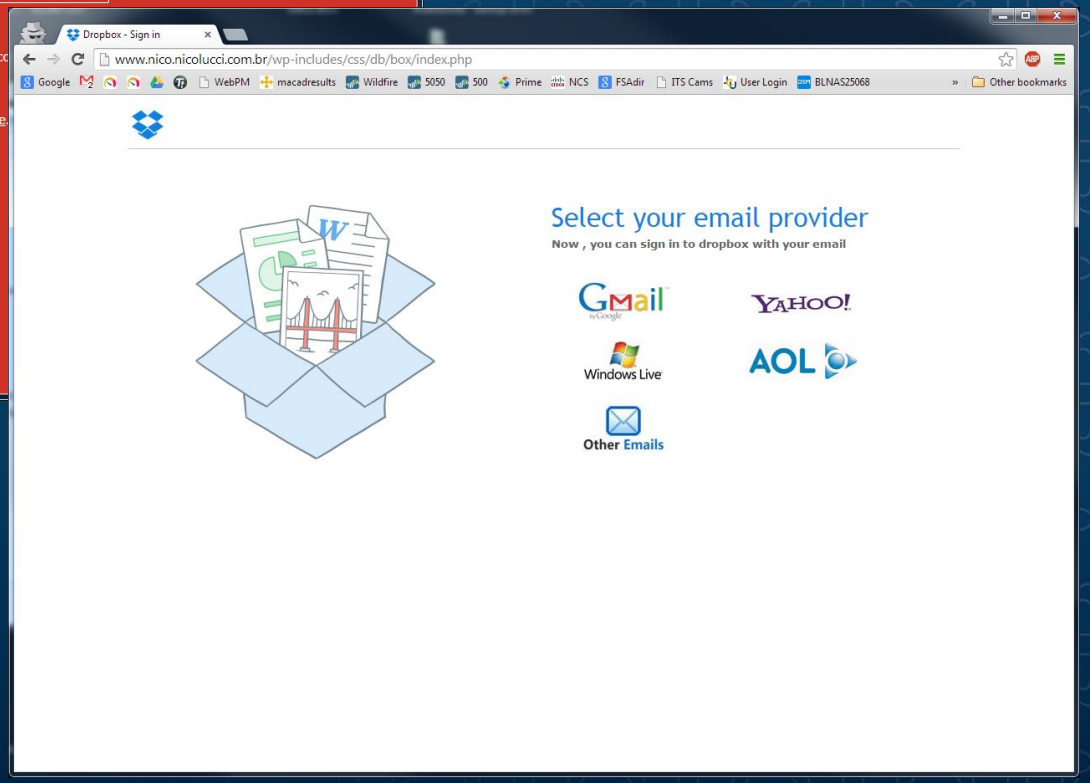
Malware "Dropbox"

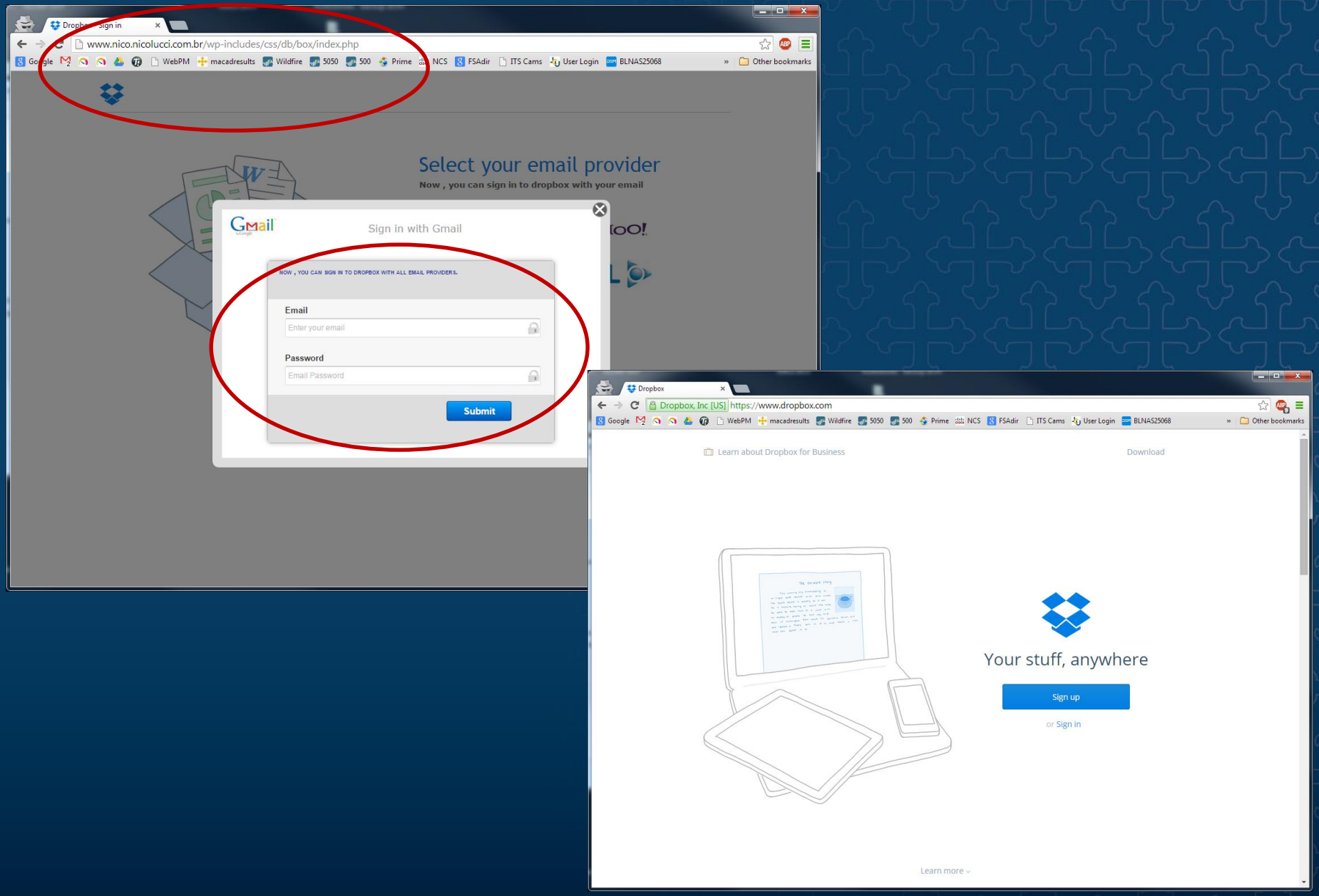


- "Now, you can sign in to dropbox with your email" – apparently any provider will do




Security error
www.nico.nicolucci.com.br/wp-includes/css/db/box/index.php
Phishing attack ahead
Attackers on www.nico.nicolucci.com.br might try to trick you to steal your information (for example, passwords, messages, or credit cards).
Hide details
Back to safety
Google Safe Browsing recently detected phishing on www.nico.nicolucci.co
sites pretend to be other websites to trick you.
If you understand the risks to your security, you may visit this infected site


Dropbox - Sign in
www.nico.nicolucci.com.br/wp-includes/css/db/box/index.php
Select your email provider
Now , you can sign in to dropbox with your email
Gmail
YAHOO!
Windows Live
AOL
Other Emails


www.nico.nicolucci.com.br/wp-includes/css/db/box/index.php
Select your email provider
Now , you can sign in to dropbox with your email
Sign in with Gmail
NOW , YOU CAN SIGN IN TO DROPBOX WITH ALL EMAIL PROVIDERS.
Email
Enter your email
Password
Email Password
Submit
Dropbox, Inc [US] https://www.dropbox.com
Learn about Dropbox for Business
Download
Your stuff, anywhere
Sign up
or Sign in
Learn more

Phishing IQ Tests

www.opendns.com/phishing-quiz

- or - if you really want to step up your game:

www.pbs.org/wgbh/nova/labs/lab/cyber

Mashable — SOCIAL MEDIA — TECH — BUSINESS — ENTERTAINMENT — WORLD — LIFESTYLE — WATERCOOLER — MORE

Social Media — FOLLOW MASHABLE >

Anonymous Hacks Syrian President's Email. The Password: 12345

8.0k SHARES

1748 Share | 4663 Tweet | 527 Share | 617 | 197 | 3

WHAT'S THIS?

BY ZOE FOX

2012-02-07 16:09:40 UTC

Syrian President Bashar al-Assad has been under fire from world leaders to step down this week. He's also under fire from hacktivist group Anonymous, who leaked hundreds of his office's emails on Monday.

While Anonymous is infamous for its hacking know-how, it doesn't take a genius computer programmer to guess one of the passwords commonly used by Assad's office accounts: 12345. The string of consecutive numbers is the second-weakest password according to a 2011 study.

Anonymous broke into the mail server of the Syrian Ministry of Presidential Affairs, accessing some 78 inboxes of Assad's staffers, according a report from Israeli daily *Haaretz*. The password 12345 was associated with several of the accounts.

Mansour Fadlallah Azzam, the minister of presidential affairs and Bouthaina Shaaban, Assad's media adviser, were among the victims of the inbox hacks.

Haaretz obtained and published one email that included documents intended to prepare the Syrian leader for his December 2011 interview with Barbara Walters. In the interview, Assad claimed the Syrian government was not killing its people.

VH1 CELEBRITY

Staff Picks: 15 MINUTES OF FAME — JARVIS IN THE ELEVATOR — WORST DRESSED — ARM CANDY

Orange Is The New Black Stars Sing *Don't Talk to Me*

Furious 7 Cast + Crew Say Goodbye To Paul Walker

Spaceballs Comes True: Syrian President's Hacked Password Was 1-2-3-4-5

hopperd | February 8, 2012 6:13 pm

To everyone who's ever been frustrated when your work email forces you to change your password every couple months, listen up, because this story is effing hilarious:

> Syrian President **Bashar al-Assad** has been under fire from world leaders to step down this week. He's also under fire from hacktivist group Anonymous, who leaked hundreds of his office's emails on Monday.
>
> While Anonymous is infamous for its hacking know-how, it doesn't take a genius computer programmer to guess one of the passwords commonly used by Assad's office accounts: 12345. The string of consecutive numbers is the second-weakest password according to a 2011 study.

That's right – the Syrian President's office literally used "1-2-3-4-5", the very same password infamously used by both **King Roland** and **President Skroob** in the movie Spaceballs *as an example of a terrible password a quarter-century ago.*

Below, watch the *Spaceballs* "combination" scene, which seemed like an exaggeration of presidential stupidity at the time:

Guess it's too late for al-Assad to update that sucker to PASSWORD?

(Thanks, **Abby**!)

Related Content

25 Most Commonly Used Passwords

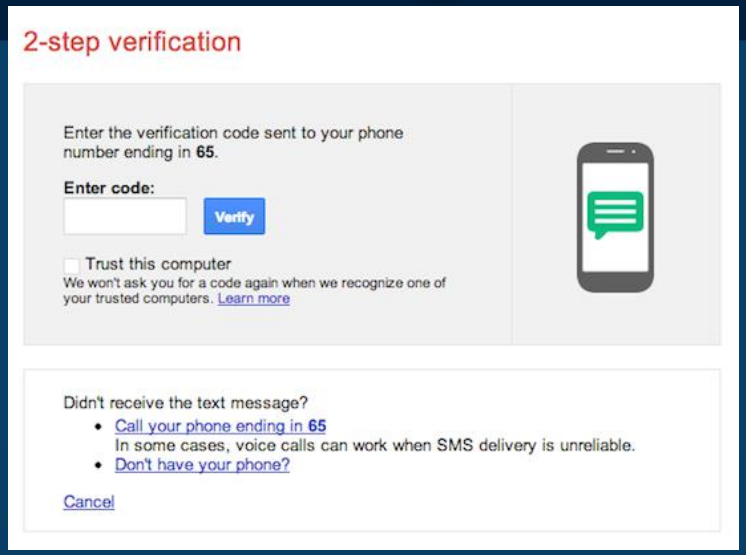
- 123456
- password
- 12345
- 12345678
- qwerty
- 123456789
- 1234
- baseball
- dragon
- football
- 1234567
- Monkey
- letmein
- abc123
- 111111
- mustang
- access
- shadow
- master
- michael
- superman
- 696969
- 123123
- batman
- trustno1

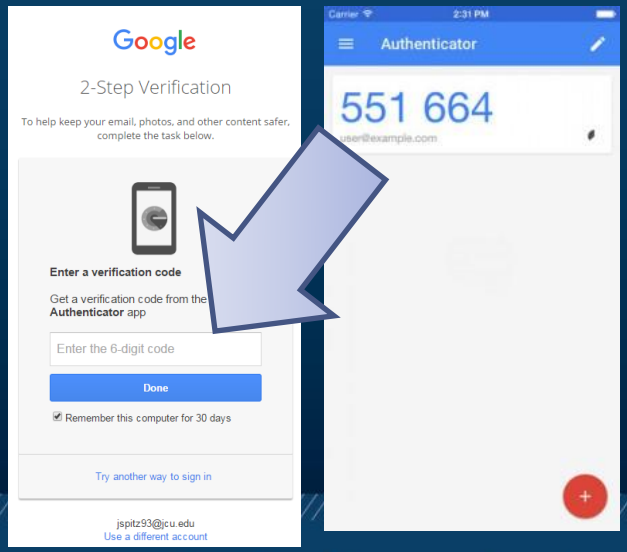
https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

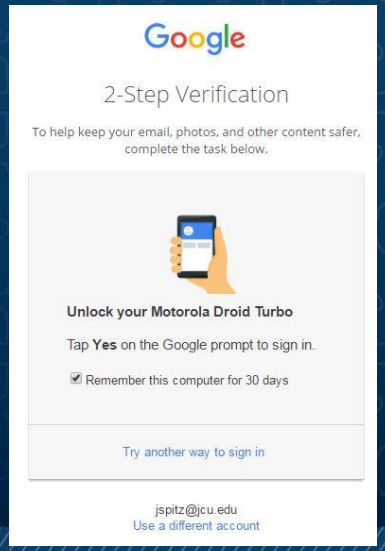
Password Best Practices

- **Use a strong password! Change periodically.**
- **Use unique passwords for each of your important accounts like email and online banking – if a criminal gains access to one, all of them could be compromised.**
- **Use a long password. The longer your password is, the harder it is to guess.**
- **Use a password with a mix of letters, numbers, and symbols.**
- **Use multi factor authentication wherever it is available.**
- Try using a phrase that only you know. For example: $3forthepiratehat
- Password Checker Demo: https://sites.jcu.edu/webapps/password/
- https://www.passworddragon.com/password-vs-passphrase

Google "2-Step Verification"







Google at JCU by the Numbers

- **17750** Accounts
- **350** were found to be, or believed to be compromised by JCU ITS or Google between October 16, 2014 and October 18, 2016
- How many people have enabled multi factor authentication?

231

5 Take Aways

1. STOP | THINK | CONNECT™
   - If you're not 100% sure, **DON'T CLICK!** If it doesn't 'feel' right, it's because it probably isn't.
2. Practice Password Diligence
3. JCU **Will NOT** ask your for your personal information! BTW, we now have unlimited Google storage for Gmail, Google Apps, and other files you want to store using Google.
4. Once you've fallen prey – you will almost always be targeted again.
5. Important stuff is sent via USPS Registered Mail.