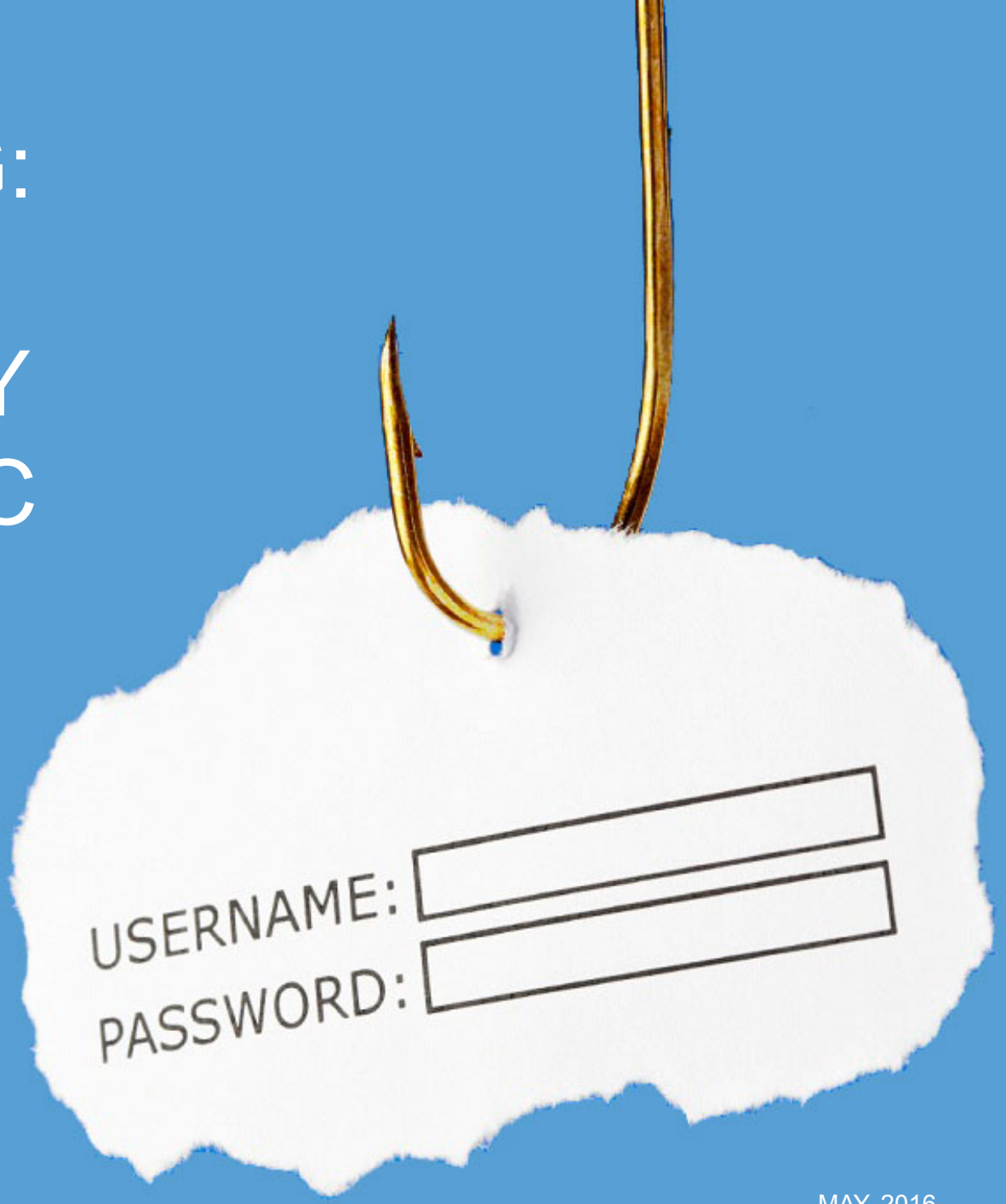
PHISHING: CYBER SECURITY PANDEMIC



UNC
INFORMATION
TECHNOLOGY SERVICES

MAY, 2016

Anthem. BlueCross BlueShield

Shop For Insurance

TECHNOLOGY

Sony Says PlayStation Hacker Got Personal Data

By NICK BILTON and BRIAN STELTER APRIL 26, 2011

Sta

ortable game console had

. So when his parents got

y on April 18, he was

NSA Details Chinese Cyber Theft of F-35, Military Secrets

Chinese hackers pillaged U.S. defense, contractor networks for critical data

SHARE TWEET EMAIL

BY: Bill Gertz Follow @BillGertz

government and private contractors.

SECURITY WEEK

INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 20

Try RSA ECAT for Endpoint Security Free for 30 Days

Detect and Block Unknown Threats

Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Manage

Home › Incident Response

Data Breach at UC Berkeley Impacts 80,000

By SecurityWeek News on February 29, 2016

Share 68 G+1 9 Tweet Recommend 12 RSS

Roughly 80,000 people might have been impacted by cyber attack that hit a UC Berkeley system containing Social Security and bank account numbers, the university warns.

UC Berkeley officials are sending alert notices to current and former faculty, staff, students and vendors after discovering that one of the university's systems had been breached, but say that there's no evidence that any personal information has been accessed, acquired, or used following the attack.

COMPUTERWORLD

NEWS

Ohio University CIO resigns in wake of data breaches

William Sams says a 'new energy level and skill set' needed

MORE

By Jaikumar Vijayan FOLLOW

Computerworld | Jul 13, 2006 1:00 AM PT

Details Emerge on Global Bank Heists by Hackers | Capitol Hill Newspapers, Once a Protected Class... | New Crowdfunding Rules Let the Small Fry Swim With... | Megyn Kelly, Contract Set to Expire Next Year, Is...

Details Emerge on Global Bank Heists by Hackers

By NICOLE PERLROTH and MICHAEL CORKERY MAY 13, 2016

UNC INFORMATION TECHNOLOGY SERVICES

By the numbers…

- On average we daily perform:
  - 400,000 reputation-based blocks
  - 170,000 signature-based blocks
  - 4,000 ad hoc customized blocks

- We block billions of additional system connection (break-in) attempts via our firewalls

Month	Total Denies	Average/day
February	2,261,922,743	77,997,336
March	2,368,550,968	76,404,870
April	2,723,784,512	90,792,817
May (not complete)	1,307,614,803	56,852,818
Feb. through April	7,354,258,223	**81,713,980**

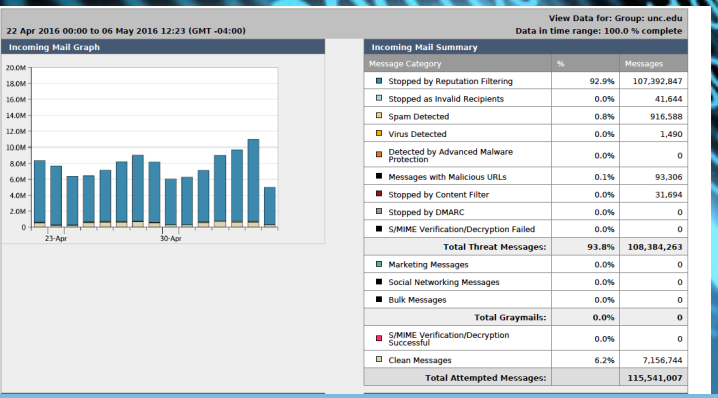
What is phishing ?

Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels.

What is spear phishing ?

Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets or military information.

- Receive 8.2 million messages each day
- Block 7.7 million messages each day (93%)
- Deliver 511,000 messages each day (7%)



22 Apr 2016 00:00 to 06 May 2016 12:23 (GMT -04:00)

View Data for: Group: unc.edu
Data in time range: 100.0 % complete

Incoming Mail Graph

Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	92.9%	107,392,847
Stopped as Invalid Recipients	0.0%	41,644
Spam Detected	0.8%	916,588
Virus Detected	0.0%	1,490
Detected by Advanced Malware Protection	0.0%	0
Messages with Malicious URLs	0.1%	93,306
Stopped by Content Filter	0.0%	31,694
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**93.8%**	**108,384,263**
Marketing Messages	0.0%	0
Social Networking Messages	0.0%	0
Bulk Messages	0.0%	0
Total Graymails:	**0.0%**	**0**
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	6.2%	7,156,744
Total Attempted Messages:		**115,541,007**

Phind the phish

"Phishing" is when email purporting to be from a legitimate source attempts to trick you into volunteering your personal or credential-related information. These messages vary in content, but all claim to be from legitimate sources such as E-Bay, your bank, PayPal, or a university group.

If you receive such a message, you should treat it as spam and simply delete it.

UNC INFORMATION TECHNOLOGY SERVICES

security.unc.edu

UNC INFORMATION TECHNOLOGY SERVICES

Many at UNC-CH are careful, so thank you!

Between March 16 and May 4 there were 4,459 phish reports to the ITS Service Desk.

There seems to be plenty of awareness and cooperation from our community.

So there is a lot of vigilance!

Yet bad actors are still using phishing effectively.

Validate Your Account

UI

UNC ITS Help Desk <helpdesk@med.unc.edu>
Monday, March 14, 2016 at 8:55 PM
To:

Dear Staff,

Due to the ongoing change in our Connect Carolina Login page, you will be require to Validate your account login to enable us integrate your account to the new login page. Please click on the Single Sign-On link below to validate your account by signing in:

http://connectcarolina.c0.pl/sso.unc.edu/idp/Authn/UserPassword/

NOTE: ENTER YOUR CORRECT ONYEN ID AND PASSWORD, AS WRONG ONYEN ID AND PASSWORD WILL AUTOMATICALLY DISABLE YOUR ACCOUNT. Failure to do this will result in permanent limited access to your mailbox.

Thank you for choosing our UNC Connect Carolina.

Regards,
UNC ADMIN VERIFICATION SERVICES

Validate Your Account

UI

UNC ITS Help Desk <helpdesk@med.unc.edu>
Monday, March 14, 2016 at 8:55 PM
To:

Dear Staff,

Due to the ongoing change in our Connect Carolina Login page, you will be require to Validate your account login to enable us integrate your account to the new login page. Please click on the Single Sign-On link below to validate your account by signing in:

http://connectcarolina.c0.pl/sso.unc.edu/idp/Authn/UserPassword/

NOTE: ENTER YOUR CORRECT ONYEN ID AND PASSWORD, AS WRONG ONYEN ID AND PASSWORD WILL AUTOMATICALLY DISABLE YOUR ACCOUNT. Failure to do this will result in permanent limited access to your mailbox.

Thank you for choosing our UNC Connect Carolina.

Regards,
UNC ADMIN VERIFICATION SERVICES
UNC ITS Help Desk | Copyright © 2016 The University of North Carolina at Chapel Hill. All rights reserved.

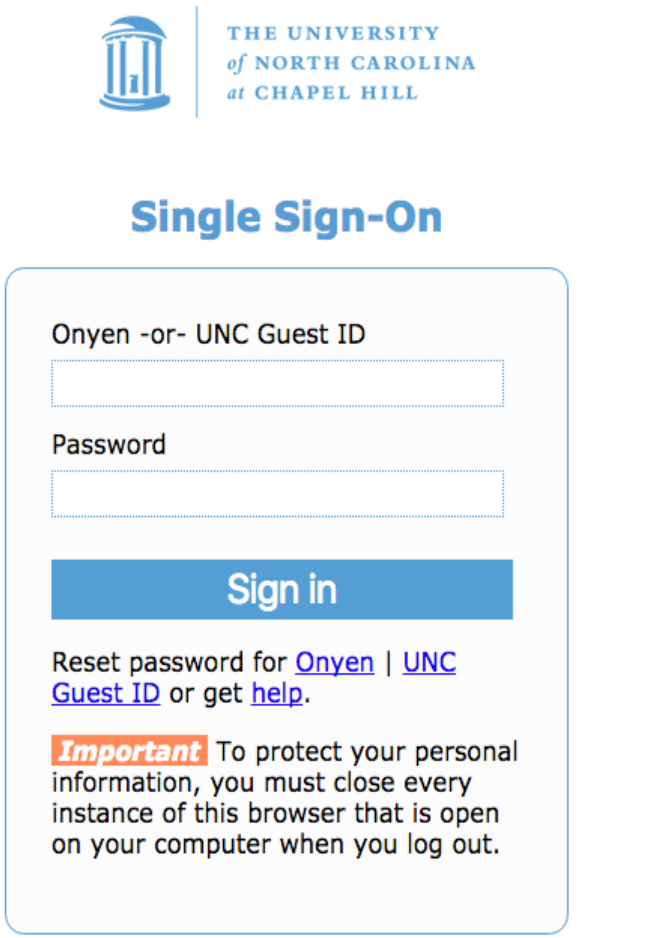
Odd opening sentence and phrasing, as well as poor capitalization. ConnectCarolina should be one word!

Suspicious URL – two many non-UNC extensions.

All caps message to create a false sense of urgency and fear.

More poor phrasing.

UNC Admin Verification Services does not exist.



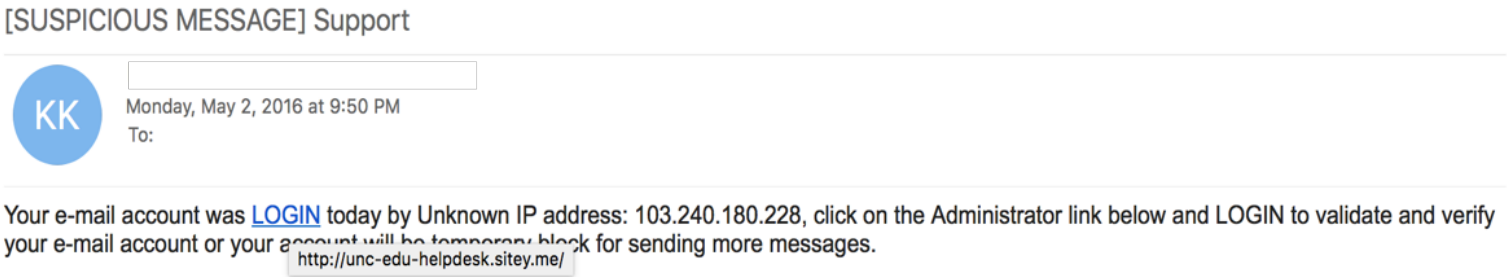

No authorized
UNC-CH
organization will
EVER ask you for
your Onyen and
password.
EVER.

What can we do about Phishing?

Understand what a phish looks like & be cautious

Report the phish: phish@unc.edu

Hover to discover the real URL destination



Hover to discover…

From: Mclaughlin, Danielle Elizabeth
Sent: Thursday, May 12, 2016 9:30 AM
To: Mclaughlin, Danielle Elizabeth <demclaug@live.unc.edu>
Subject: Warning! Your Urgent Attention Is Needed

Thank your for being part of THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL webmail Services. We're excited to contact your email!

What to do now!

We are currently updating our UNIVERSITY of NORTH CAROLINA at CHAPEL HILL services, due to this upgrade we sincerely call your attention
to follow below link and reconfirm CAROLINA at CHAPEL HILL email account details.

http://gene-korea.com/gn/data/-h/unc.edu.htm
Click or tap to follow link.

Click here to reconfirm your email account

Thank You

Hovering your mouse over a link shows the target URL destination

Additional protections

- Physical security in data centers and network wiring closets
- Encrypt data at rest
- Encrypt data in transit
- Standards based authentication
- Anti – virus
- Application firewalls
- **Outreach programs**
- **Two-factor**
- **Microsoft Advanced Threat Detection**

In phishing *you* are the fish