Rockhurst University is sued over data breach in phishing scam

Greenwich University suffers second data breach this year in apparent ‘revenge hack’ by former student

Leaked details reportedly include student grades and feedback, staff holiday details and ‘sickness table’ highlighting students with disabilities

NC State faces data breach; nearly 38,000 could be affected

DDoS Attacks Against Universities Are on the Rise

Security Breach at OU Exposes Thousands of Students’ Data

By Dana Branham, The OU Daily June 14, 2017

College of Engineering network disabled in response to sophisticated cyberattack

Kentucky State University becomes latest victim of data breach

University suffers DDoS attack after it's schooled by own IoT devices

Infected vending machines and light bulbs teach establishment a lesson

Data breach hits 63,000 U. of Central Florida students, staff

University of Virginia data breach exposed financial data

The university has admitted that cyberattackers were able to infiltrate areas of the human resource department's network.

Data Breach At UC Berkeley Could Affect 80,000 People

Around half of all students could potentially be affected by the breach, which was carried out by an unknown hacker.

University emailed hundreds of students revealing who needed extensions for suicidal thoughts

University employees vulnerable after tax data breach

April 12, 2016 0 Comments
University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.
Agenda

Discuss UVM Targets

Why it matters

What you can do

How to get help
Email Averages:
Messages Received
700K - 1 Million per Day
45% Filtered Immediately
15% Flagged as SPAM

Incidents:
User Account Compromises:
**** in 2016

Breaches:
**** State Reportable Breaches

**** See Information Security Officer for details
What are they after?

Electronic Theft

Identity Theft

Ransom

Healthcare Fraud

UVM Resources
UVM Resources

- Send Thousands of SPAM Email
- Compromise Websites
  - Host Unwanted Site Links
  - Host Malware
- Attack Other Resources or Organizations
“Information Security is Everyone’s Responsibility”
3. General Responsibilities for University Employees

University Employees have special responsibilities because of the access they have to University Information and University Information Systems. Each University Employee is expected to know and understand the security requirements of the types of University Information with which they work and to take measures to protect it in accordance with the Procedures.
Email Awareness
Malicious Emails

Credential Harvesting
Payload Delivery
Information Disclosure
https://webauth.uvm.edu/webauth/
UVM Computing <[redacted]@albany.edu>

Wednesday, March 15, 2017 at 6:44 PM
To: [redacted]

This email has been sent to: [redacted]@uvm.edu

Our systems have detected an unusual high volume email traffic from this email address in the past few hours.

Email sent from: [redacted]@uvm.edu

Total Email sent in 24hrs: 5,393

Time: 3/15/2017 4:44:02 p.m.

IP address: 202.43.188.19

Country: Indonesia

We believe this is not you sending these unsolicited emails. We have reason to believe that, this email is no longer in use and an email virus has taken over your computer. Therefore, we shall pass this message around a few times and afterwards, suspend access to this email address and terminate this service to quarantine this activity.

What To Do?

If you believe that, this is an error and this email is still being actively used you, please click HERE to login and verify this request.

Your email would be removed from the delete queue and subsequent information will be passed on to you. We have teamed up with the Microsoft Digital Crimes Unit (DCU) to enhance your security

System Ethics and Compliance Officer
Mail Administration | IT Solutions
THE UNIVERSITY OF VERMONT - BURLINGTON, VT 05405
Verify your email address - Code 18246353

UVM Computing <UVM Computing@uvm.edu>
Wednesday, March 15, 2017 at 6:44 PM
To: [Redacted]

This email has been sent to: [Redacted]

Our systems have detected an unusual high volume email traffic from this email address.

Email sent from: [Redacted]

Total Email sent in 24hrs: 5,393
Time: 3/15/2017 4:44:02 p.m.
IP address: 202.43.188.19
Country: Indonesia

We believe this is not you sending these unsolicited emails. We have reason to believe that, this email is no longer in use and an email virus has taken over your computer. Therefore, we shall pass this message around a few times and afterwards, suspend access to this email address and terminate this service to quarantine this activity.

What To Do?

If you believe that; this is an error and this email is still being actively used you, please click HERE to login and verify this request.

Your email would be removed from the delete queue and subsequent information will be passed [Redacted] to enhance your security.

------------------------------------------------------------
System Ethics and Compliance Officer
Mail Administration | IT Solutions
THE UNIVERSITY OF VERMONT - BURLINGTON, VT 05405

[IT] University Mailbox Quota Exceeded!

UVM Tech Desk <Toth.Nikolett@uni-nke.hu>

Sunday, July 16, 2017 at 1:49 PM
To: Public Health

This message is high priority.

Your university mailbox quota has exceeded its limit, you may not be able to send/receive more emails.

Please delete any item you don’t need from your mailbox and empty your Deleted Items folder OR FOLLOW HERE to enable automatic increase your mailbox storage.

The office of Information Security will keep this updated if information should change, but we encourage all users to run their updates after the expected release of this patch.

With kind regards,
Your UVM Tech Team

The University of Vermont

---
The University of Vermont
Information Technology (IT)

© 2017 Information Technology (IT). All rights reserved.
IT University Mailbox Quota Exceeded!

UVM Tech Desk <toth.nikolett@uni-nke.hu>
Sunday, July 16, 2017 at 1:49 PM
To: Public Health

This message is high priority.

Your university mailbox quota has exceeded its limit, you may not be able to send/receive more emails.

Please delete any item you don't need from your mailbox and empty your Deleted Items folder OR FOLLOW HERE to enable automatic increase your mailbox storage.

The office of Information Security will keep this updated if information should change, but we encourage all users to check their mailbox after the expected release of this patch.

With kind regards,
Your UVM Tech Team

http://www.webauth-uvm.ml/
• Consider what messages are available in your email.

• Consider who you are emailing.

• Consider where you are storing your email messages.
• Understand the data in your files

• Know where your files are stored.

• Understand how they are protected

• Use Encryption
Access

- Do not share your passwords
- Use unique passwords
- Only give access to those that need it
- Don’t leave sensitive info in plain sight
- Report issues/concerns
• Protect your devices – Lock them up!

• Keep the software up to date.

• Utilize University supported tools and services.
Who you gonna call?
Information Security Office
234 Waterman Building

iso@uvm.edu

Breach Notification - 866-236-5752
Phishing Emails - abuse@uvm.edu
https://www.uvm.edu/it/security/

The University of Vermont