A SENSITIVE DATA PROTECTION STRATEGY

Randy Marchany
VA Tech IT Security Office & Lab
marchany@vt.edu
https://security.vt.edu
Twitter: @randymarchany

YOU ARE A TARGET

SANS SECURING THE HUMAN

Username & Passwords

Once hacked, cyber criminals can install programs on your computer that capture all your keystrokes, including your username and password. That information is used to log into your online accounts, such as:

- *Your bank or financial accounts, where they can steal or transfer your money.*
- *Your iCloud, Google Drive, or Dropbox account where they can access all your sensitive data.*
- *Your Amazon, Walmart or other online shopping accounts where they can purchase goods in your name.*
- *Your UPS or Fedex accounts, where they ship stolen goods in your name.*

Email Harvesting

Once hacked, cyber criminals can read your email for information they can sell to others, such as:

- *All the names, email addresses and phone numbers from your contact list.*
- *All of your personal or work email.*

Virtual Goods

Once hacked, cyber criminals can copy and steal any virtual goods you have and sell them to others, such as:

- *Your online gaming characters, gaming goods or gaming currencies.*
- *Any software licenses, operating system license keys, or gaming licenses.*

Botnet

Once hacked, your computer can be connected to an entire network of hacked computers controlled by the cyber criminal. This network, called a botnet, can then be used for activities such as:

- *Sending out spam to millions of people.*
- *Launching Denial of Service attacks.*

You may not realize it, but you are a target for cyber criminals. Your computer, your mobile devices, your accounts and your information all have tremendous value. This poster demonstrates the many different ways cyber criminals can make money by hacking you. Fortunately, by taking some simple steps, you can help protect yourself and your family. To learn more, subscribe to OUCH!: a security newsletter designed to help people just like you.

www.securingthehuman.org/ouch

Identity Hijacking

Once hacked, cyber criminals can steal your online identity to commit fraud or sell your identity to others, such as:

- *Your Facebook, Twitter or LinkedIn account.*
- *Your email accounts.*
- *Your Skype or other IM accounts.*

Web Server

Once hacked, cyber criminals can turn your computer into a web server, which they can use for the following:

- *Hosting phishing websites to steal other people's usernames and passwords.*
- *Hosting attacking tools that will hack people's computers.*
- *Distributing child pornography, pirated videos or stolen music.*

Financial

Once hacked, cyber criminals can scan your system looking for valuable information, such as:

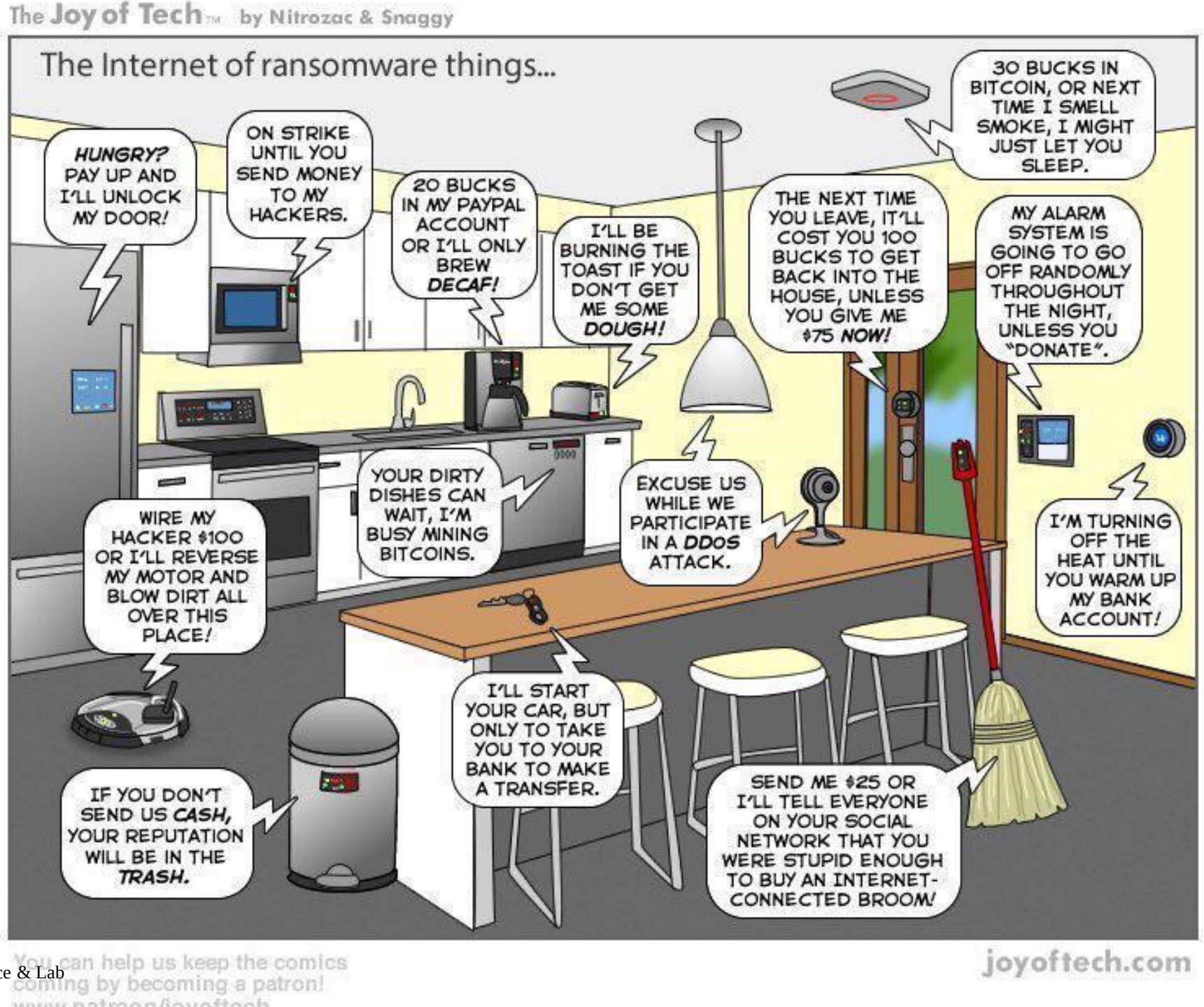
- *Your credit card information.*
- *Your tax records and past filings.*
- *Your financial investments and retirement plans.*

Extortion

Once hacked, cyber criminals can take over your computer and demand money. They do this by:

- *Taking pictures of you with your computer camera and demanding payment to destroy or not release the pictures.*
- *Encrypting all the data on your computer and demanding payment to decrypt it.*
- *Tracking all websites you visit and threatening to publish them.*

This poster is based on the original work of Brian Krebs. You can learn more about cyber criminals at his blog at http://krebsonsecurity.com


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UNTIL YOU SEND MONEY TO MY HACKERS.
20 BUCKS IN MY PAYPAL ACCOUNT OR I'LL ONLY BREW DECAF!
I'LL BE BURNING THE TOAST IF YOU DON'T GET ME SOME DOUGH!
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
YOUR DIRTY DISHES CAN WAIT, I'M BUSY MINING BITCOINS.
EXCUSE US WHILE WE PARTICIPATE IN A DDOS ATTACK.
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'LL START YOUR CAR, BUT ONLY TO TAKE YOU TO YOUR BANK TO MAKE A TRANSFER.
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
SEND ME $25 OR I'LL TELL EVERYONE ON YOUR SOCIAL NETWORK THAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech
joyoftech.com


1 2 3
4 5 6
7 8 9
* 0 #

MEET A SPAMMER

Hacker sends anti-Semitic...

The Washington Post (WP Compan... (US) https://www.washingtonpost.com/news/

Search

Sections

The Washington Post

Sign In Subscribe

More

Grade Point

Hacker sends anti-Semitic fliers to network printers at Princeton, many other colleges

A 89 Save for Later Reading List

By Mary Hui and Susan Svrluga March 29 Follow @SusanSvrluga

Princeton University. (Associated Press)

PRINCETON, N.J. — A notorious white supremacist computer hacker has claimed responsibility for sending anti-Semitic fliers to networked printers at several universities across the country, a coordinated cyberattack that

Most Read

1 A huge tornado killed his wife and destroyed their home. He filmed the whole thing.

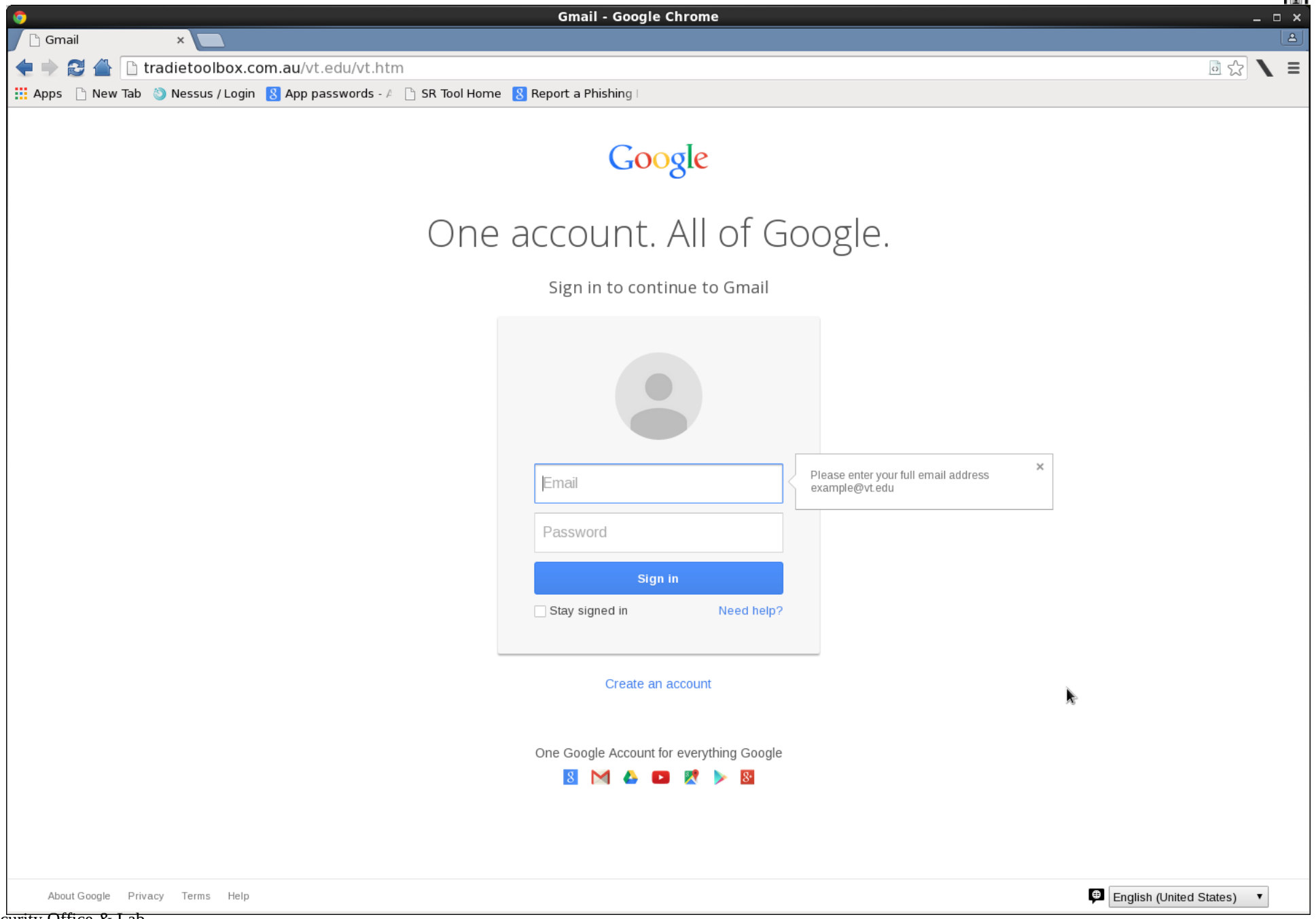
2 9-year-old reporter breaks crime news, posts videos, fires back at critics

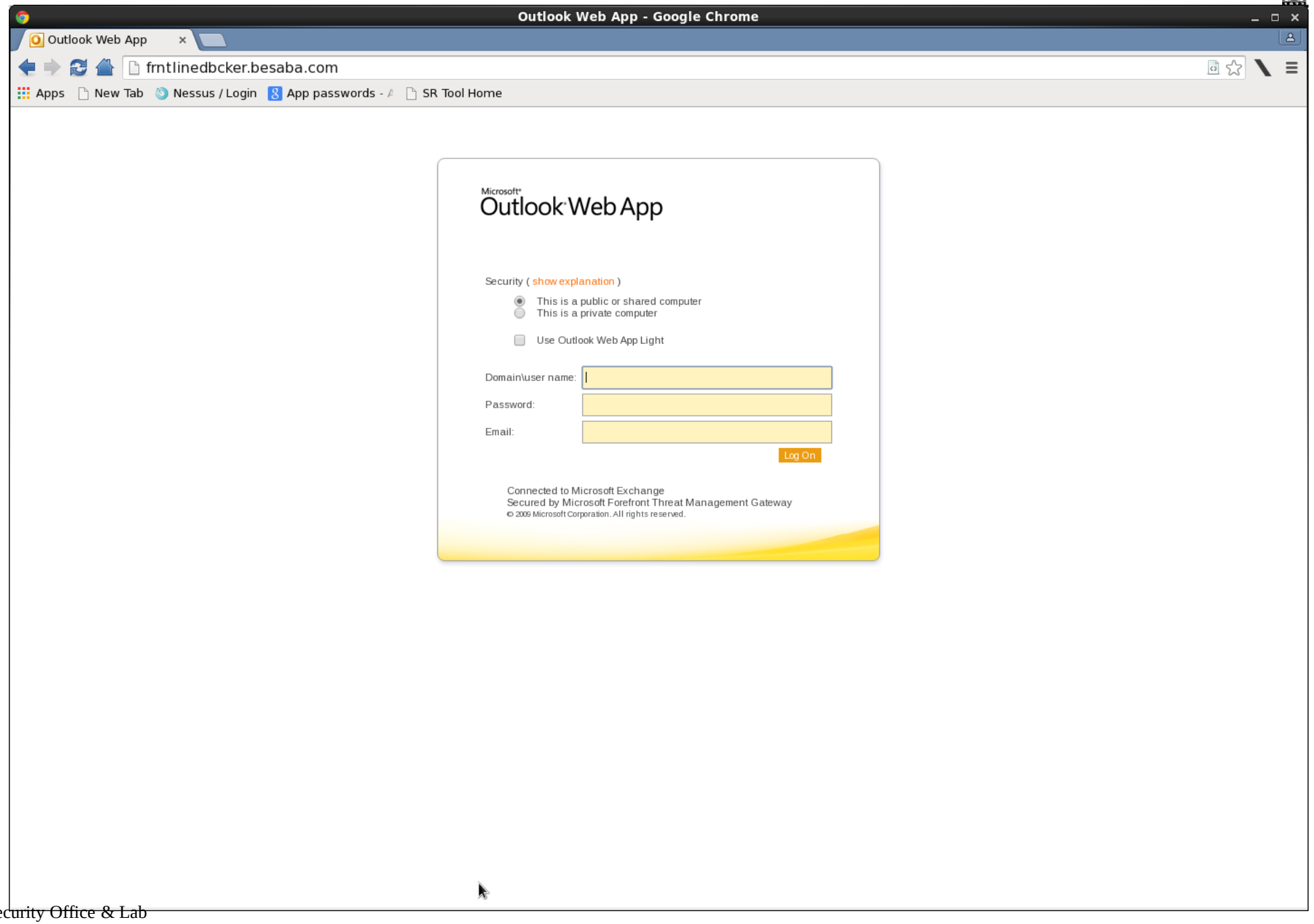
3 George Mason U. changes name of Scalia law school to avoid embarrassing acronyms

4 Yes, it may snow a bit in D.C. Saturday, as polar vortex unleashes parting blow

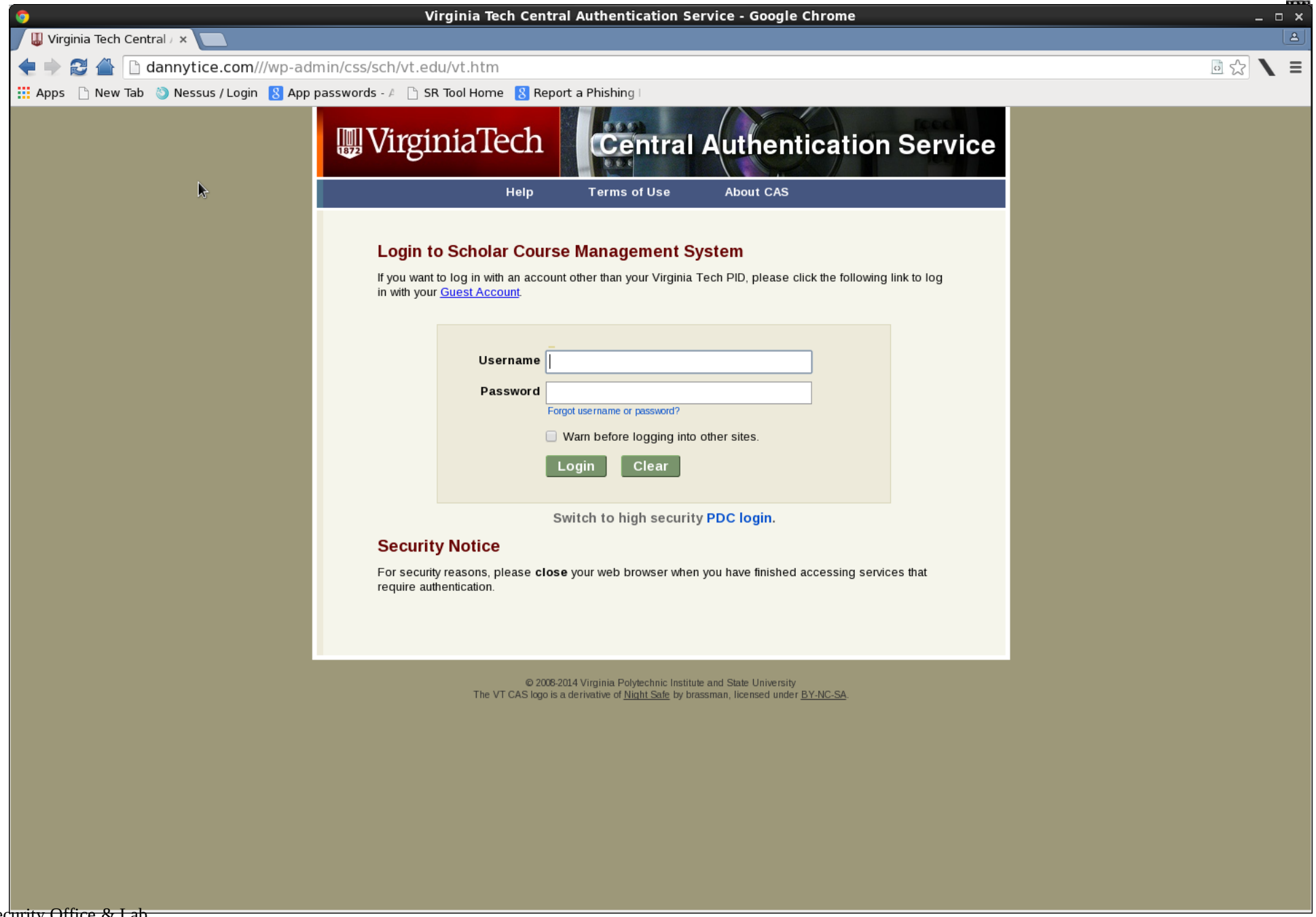
5 Maryland board approves $5.6-billion Purple Line contract

Unlimited Access to The Post. **Just 99¢**

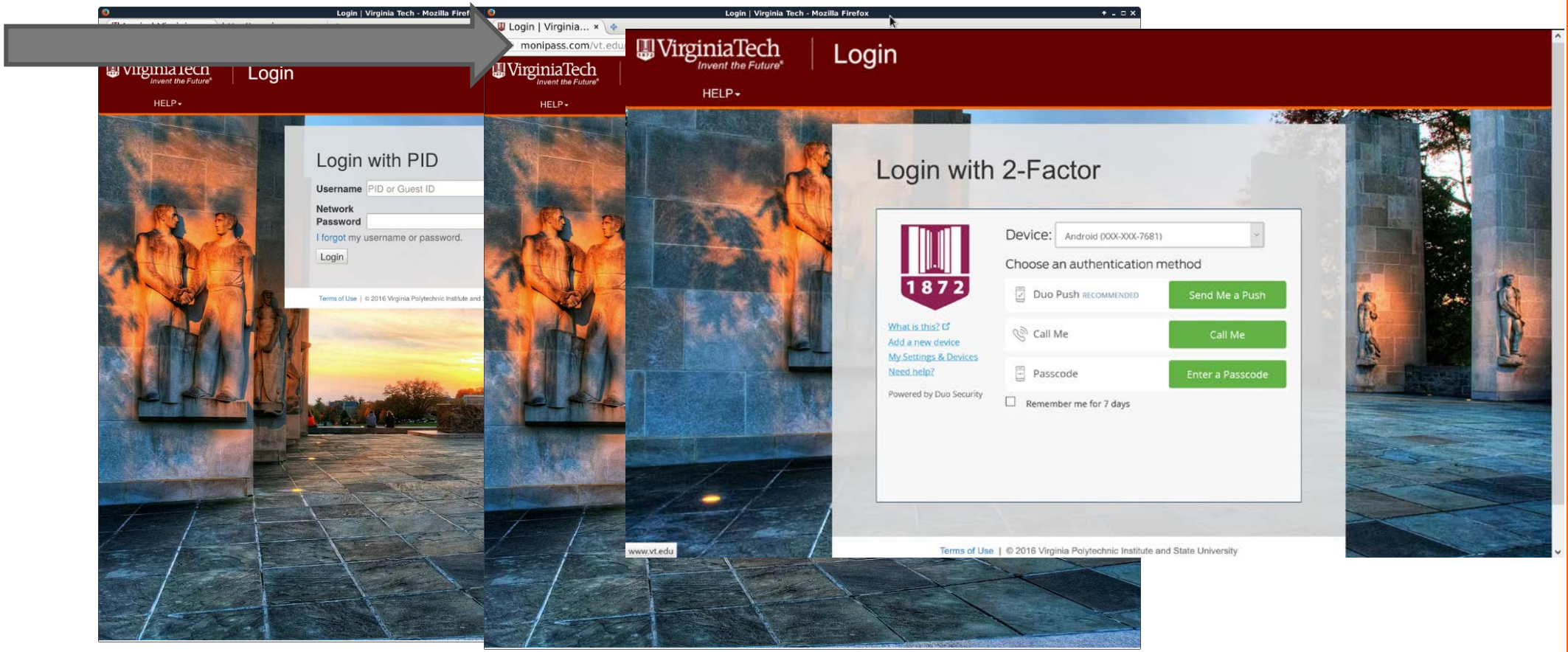

Gmail - Google Chrome
Gmail
tradietoolbox.com.au/vt.edu/vt.htm
Apps
New Tab
Nessus / Login
App passwords -
SR Tool Home
Report a Phishing
Google
One account. All of Google.
Sign in to continue to Gmail
Email
Password
Sign in
Stay signed in
Need help?
Please enter your full email address
example@vt.edu
Create an account
One Google Account for everything Google
About Google
Privacy
Terms
Help
English (United States)


Outlook Web App - Google Chrome
Outlook Web App
frntlinedbcker.besaba.com
Apps
New Tab
Nessus / Login
App passwords -
SR Tool Home
Microsoft
Outlook Web App
Security (show explanation)
This is a public or shared computer
This is a private computer
Use Outlook Web App Light
Domain\user name:
Password:
Email:
Log On
Connected to Microsoft Exchange
Secured by Microsoft Forefront Threat Management Gateway
© 2009 Microsoft Corporation. All rights reserved.

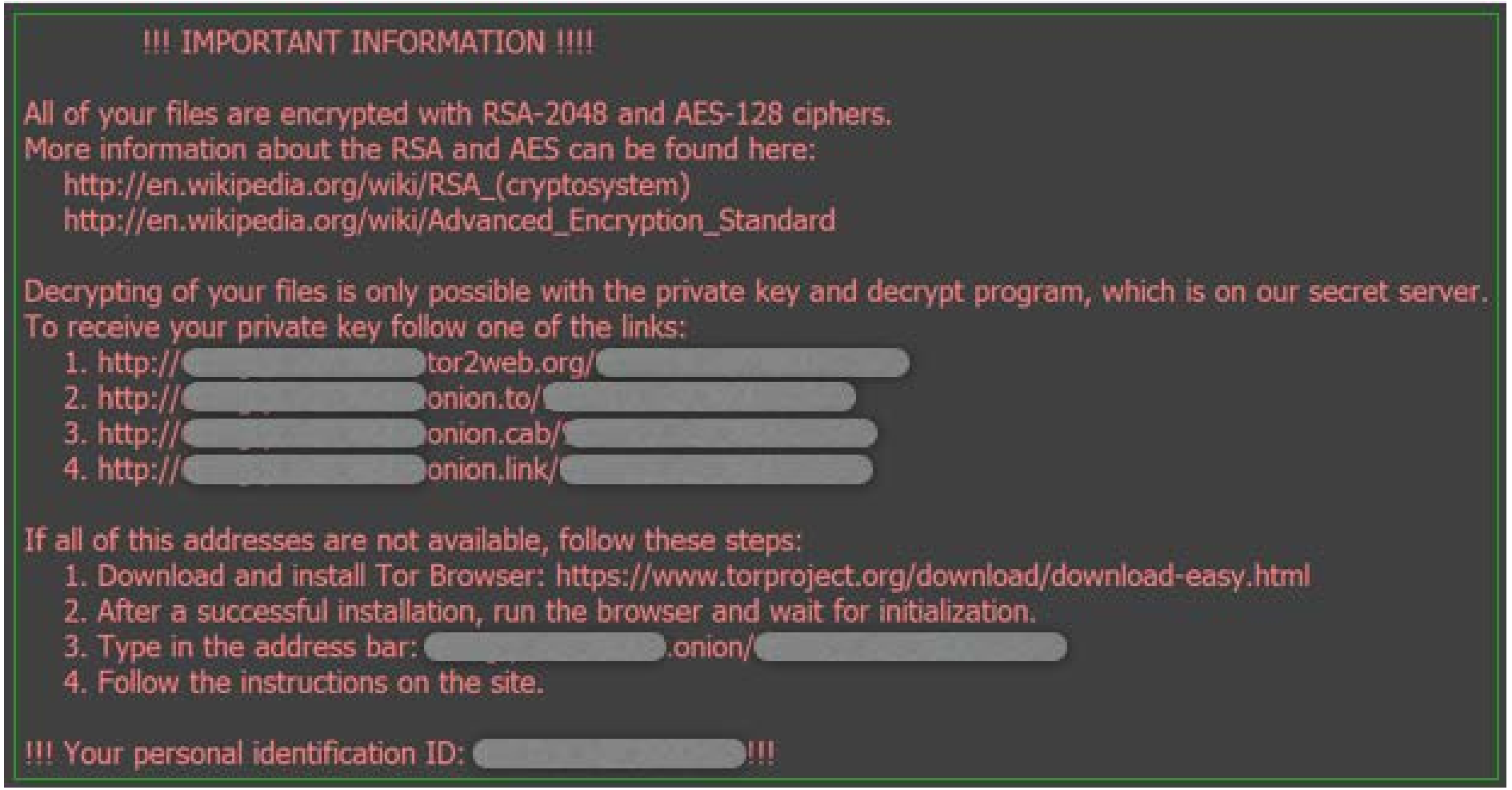

VirginiaTech
Central Authentication Service
Help
Terms of Use
About CAS
Login to Scholar Course Management System
If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your Guest Account.
Username
Password
Forgot username or password?
Warn before logging into other sites.
Login
Clear
Switch to high security PDC login.
Security Notice
For security reasons, please close your web browser when you have finished accessing services that require authentication.


Virginia Tech Central Authentication Service - Google Chrome
Virginia Tech Central
dannytice.com///wp-admin/css/sch/vt.edu/vt.htm
Apps
New Tab
Nessus / Login
App passwords -
SR Tool Home
Report a Phishing
VirginiaTech
Central Authentication Service
Help
Terms of Use
About CAS
Login to Scholar Course Management System
If you want to log in with an account other than your Virginia Tech PID, please click the following link to log in with your Guest Account.
Username
Password
Forgot username or password?
Warn before logging into other sites.
Login
Clear
Switch to high security PDC login.
Security Notice
For security reasons, please close your web browser when you have finished accessing services that require authentication.
© 2008-2014 Virginia Polytechnic Institute and State University
The VT CAS logo is a derivative of Night Safe by brassman, licensed under BY-NC-SA.

IS IT REAL OR FAKE, PART 2



“LOCKY” RANSOMWARE



NO REALLY… WHAT IS A DNS FIREWALL?

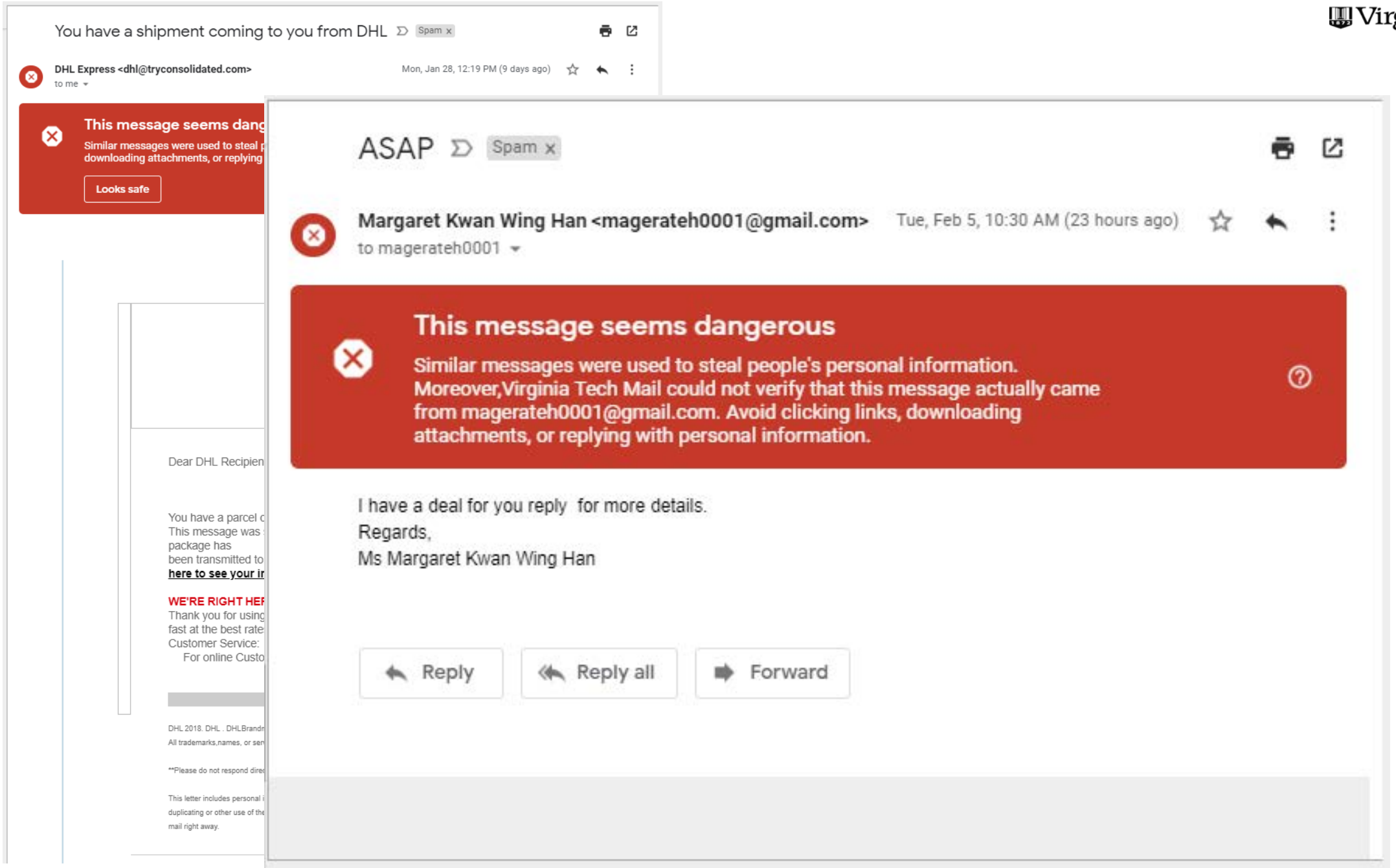
Also known as Response Policy Zone (RPZ).

Goal is to protect clients from malicious domains.

English translation: If you click on a link, the site is checked against a list of "bad/evil" domains. If it's there, the DNS server says "host not found". This helps protect you from getting to a bad site. The list is updated daily.

VT has been experimenting with RPZ since 2012.

This service went online for everyone on campus on 3/11/2019.


You have a shipment coming to you from DHL
Spam x
DHL Express <dhl@tryconsolidated.com>
to me
Mon, Jan 28, 12:19 PM (9 days ago)
This message seems dang
Similar messages were used to steal p
downloading attachments, or replying
Looks safe
Dear DHL Recipien
You have a parcel c
This message was
package has
been transmitted to
here to see your ir
WE'RE RIGHT HER
Thank you for using
fast at the best rate
Customer Service:
For online Custo
DHL 2018. DHL . DHLBrandr
All trademarks,names, or ser
**Please do not respond direc
This letter includes personal i
duplicating or other use of the
mail right away.
ASAP
Spam x
Margaret Kwan Wing Han <magerateh0001@gmail.com>
to magerateh0001
Tue, Feb 5, 10:30 AM (23 hours ago)
This message seems dangerous
Similar messages were used to steal people's personal information.
Moreover,Virginia Tech Mail could not verify that this message actually came
from magerateh0001@gmail.com. Avoid clicking links, downloading
attachments, or replying with personal information.
I have a deal for you reply for more details.
Regards,
Ms Margaret Kwan Wing Han
Reply
Reply all
Forward

PASSWORD MANAGEMENT

DON'T SHARE YOUR PASSWORD!

If a person does something malicious while logged on as you, it will likely be blamed on you

If you think someone knows your password – CHANGE IT!

SELECTING GOOD PASSWORDS

General Password form: N|Word|Sym (1Monkey!)

General form: CVCCVC, where C=consonant, V=Vowel

1!Soccer

Summer1!

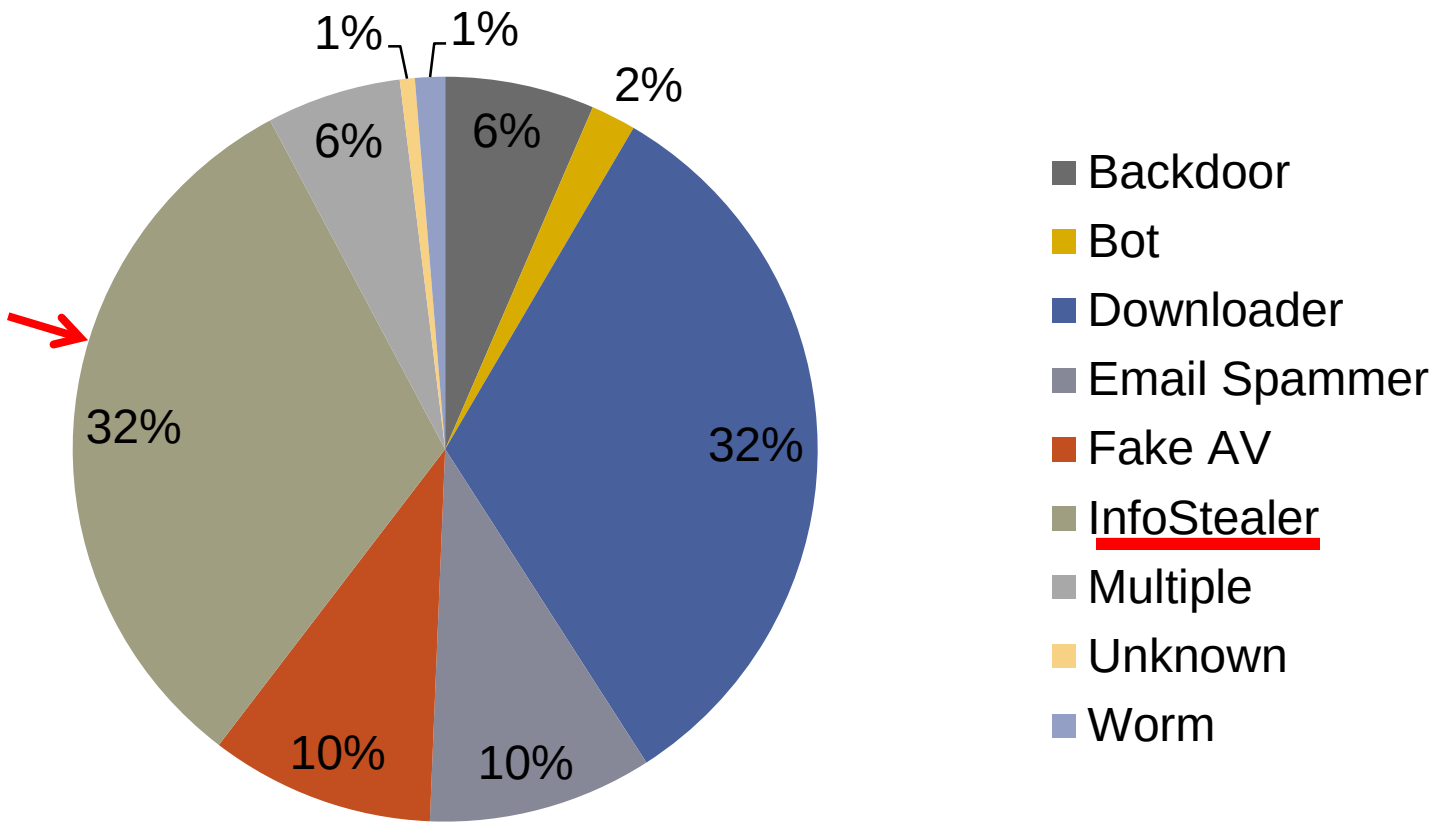
HotDog2017!

Use passphrases: "Pay no attention to the man behind the curtain,"

- A special event: "I went to Ft. Lauderdale in 85!"

Length is more important than complexity

MALWARE BY TYPE



WHAT CAN HAPPEN?

IP 128.173.136.144.4585 > 79.137.237.76.80: tcp 525

E..5..@.}.....O..L...P.....z.P....N.....

.....0.O....(

.....@.....X.....d...#.....CPSRE01_E4A1565C3FC0958Eiexplore.exehttps://auth.vt.edu/login?service=https://solutions.sciq[redacted]Auth/NetId?OrgName (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; GTB7.2; InfoPath.2; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; .NET4.0C)username: topdj

password: M@r21odd1

lt: LT-214538-dxGMamhM0vggzg1z4b4cIIrYhnX3L5

execution: e3s1

_eventId: submit

submit: Login

SENSITIVE DATA PROTECTION STRATEGY

- **Create data management framework**
- **Create data classification framework**

- **Create Sensitive Data Search framework**
- **Create Sensitive Data Protection framework**

- **Create Sensitive Data Breach framework**

Protecting Sensitive Data

Keeping sensitive data safe from inappropriate access and disclosure is of the utmost importance. Virginia Tech has many policies, procedures, and standards in place to protect sensitive data. It is the responsibility of everyone handling sensitive data from Virginia Tech to be familiar with these policies, procedures, and standards. It is important to find out what sensitive data you are handling and what steps are needed to protect it.

Where to start?

There are 6 specific data elements that Virginia Tech has protected with the "**Standard for Transmitting and Storing Personally Identifying Information**". The data elements covered under this standard include:

- Social Security number
- Credit card number
- Debit card number
- Bank account number
- Driver's license number
- Passport number

Why might I have this data?

Virginia Tech does not typically use Social Security numbers in its daily operations. It is important to recall that Virginia Tech formerly used Social Security numbers as identification numbers. What files might you have that would contain the "old ID numbers?"

- Personnel files?
- Student work or student grade files?
- Accounts receivable files?
- Have you ever stored credit (or debit) card numbers? Did you make travel arrangements for yourself or others that may have included such information? Have you made purchases where storing such a number may have occurred?
- Arranging travel may also have led to recording and storing passport numbers—check likely places.
- Are any of these files defined-as-originals that must be kept for a defined period of time? Has that period of time expired? If so, remove them. If not, where can these data be kept

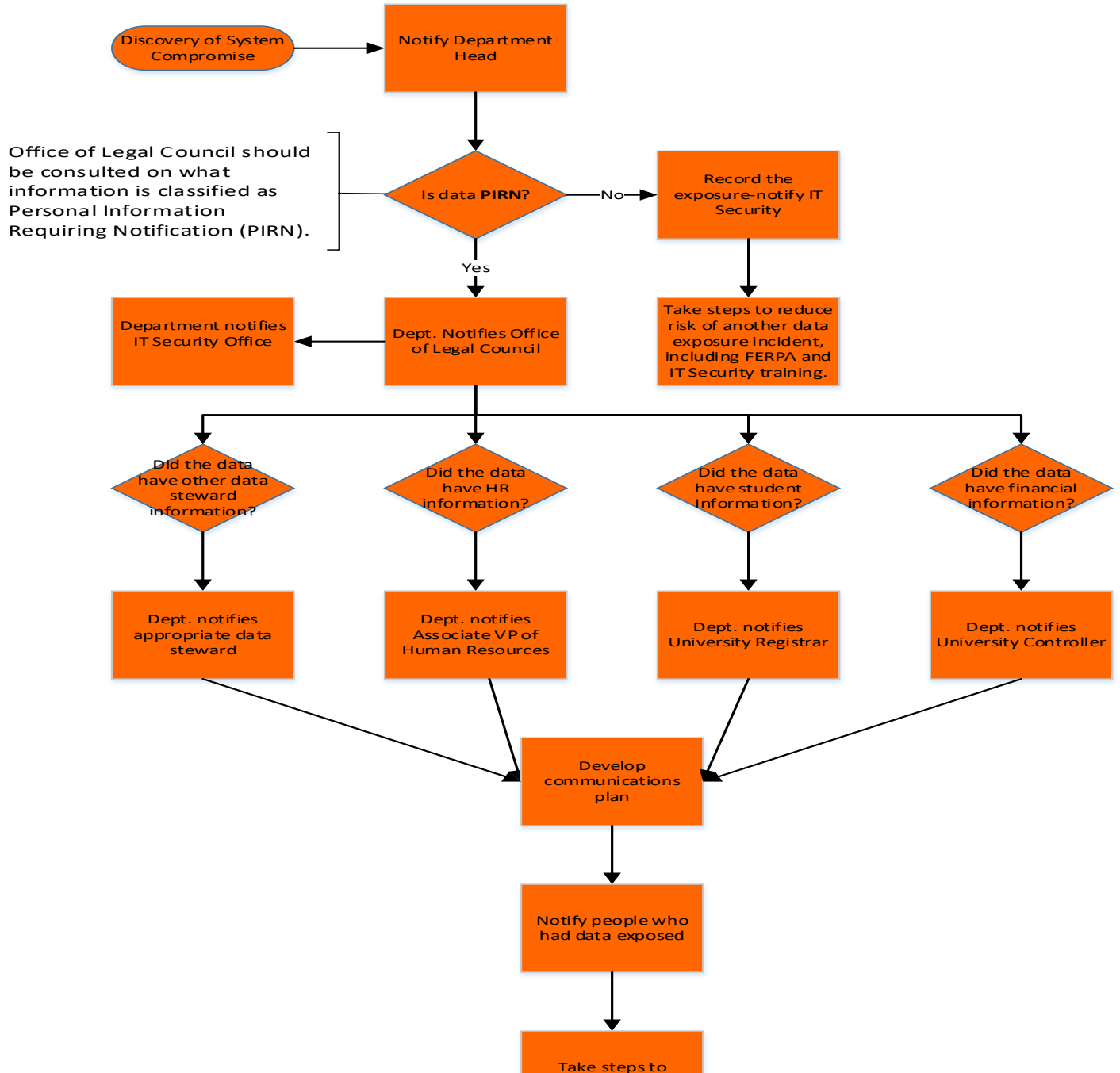
Related Pages:

Identity Finder

Find_SSNs

Rights Management Services

VeraCrypt


Discovery of System Compromise
Notify Department Head
Office of Legal Council should be consulted on what information is classified as Personal Information Requiring Notification (PIRN).
Is data PIRN?
No
Record the exposure-notify IT Security
Yes
Department notifies IT Security Office
Dept. Notifies Office of Legal Council
Take steps to reduce risk of another data exposure incident, including FERPA and IT Security training.
Did the data have other data steward information?
Did the data have HR information?
Did the data have student Information?
Did the data have financial information?
Dept. notifies appropriate data steward
Dept. notifies Associate VP of Human Resources
Dept. notifies University Registrar
Dept. notifies University Controller
Develop communications plan
Notify people who had data exposed
Take steps to

VA DATA BREACH NOTIFICATION LAWS

§ 2.2-3806. Rights of data subjects.

A. Any agency maintaining personal information shall:

Give notice to a data subject of the possible dissemination of part or all of this information to another agency, nongovernmental organization or system not having regular access authority, and indicate the use for which it is intended, and the specific consequences for the individual, which are known to the agency, of providing or not providing the information.

DATA MANAGEMENT FRAMEWORK

No one gets access to data w/o Data Owner approval

- Data Owners/Trustee
- Data Steward
- Data Expert

Example: www.policies.vt.edu/7100.pdf

DATA TRUSTEES, STEWARDS, EXPERTS

Data trustees

senior university officials, typically a vice president, who have planning and policy-making responsibilities for university data

Data stewards

assigned by data trustees. Data stewards classify data for access and sensitivity, define and monitor data quality. They are the primary contact points for members of the university community who may have concerns with data.

Data experts and data managers

specified by Policy 7100 and typically have internal office responsibilities under the direction of a data steward.

https://policies.vt.edu/7100.pdf

DATA CLASSIFICATION FRAMEWORK

HIGH RISK

Protection of the data is required by law/regulation and

Virginia Tech is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed

The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Data level determines security level of asset storing the data

Data in Transit, Data at Rest

REGULATION COMPLIANCE

FERPA – mandates appropriate security of the education record

HIPAA - privacy protection for health records

G-L-B - the security and confidentiality of customer nonpublic financial information records

ITAR – International Traffic & Arms Regulations – export controlled research or data

Patriot Act – gives the federal government the ability to investigate threats to the national security

Copyright laws – legal right to exclusive publication, production, sale, or distribution of literary, musical or artistic work

Additional Federal and State regulations – dealing with day-to-day activities from purchasing items to personnel issues to reporting structures to what's legal to access

COMPLIANT

SECURE!

DATA SEARCH FRAMEWORK

Have to find the data before you can protect it

Commercial or Freeware

Spirion (former IdentityFinder), Find_SSN (Freeware)

Run on ALL systems

Do you need this data for your job

yes? Encrypt at rest, in transit

no? Delete the file

WHERE MIGHT IT BE?

Personnel files?

Student work or student grade files?

Accounts receivable files?

Have you ever stored credit (or debit) card numbers? Did you make travel arrangements for yourself or others that may have included such information? Have you made purchases where storing such a number may have occurred?

Arranging travel may also have led to recording and storing passport numbers—check likely places.

Are any of these files defined-as-originals that must be kept for a defined period of time? Has that period of time expired? If so, remove them. If not, where can these data be kept more securely?

Data Protection Framework

IMPORTANT POLICES

1060 Policy on Social Security Numbers
7000 Acceptable Use of Computer and Communication Systems
7010 Policy for Securing Technology resources and Services
7025 Safeguarding Nonpublic Customer Information
7030 Policy on Privacy Statements on Virginia Tech Web Sites
7035 Privacy Policy for employees Electronic Communications
7040 Personal Credentials for enterprise Electronic Services
7100 Administrative Data Management and Access Policy
7200 University IT Security Program
7205 IT Infrastructure, Architecture and Ongoing Operations
7210 IT Project Management
7215 IT Accessibility

or visit https://it.vt.edu/resources/policies.html

BYOD

VA Tech has been in BYOD since 1984

Student required to own computer

Use ISP security model

Protect the data first then the device

who cares where PII is stored if it's encrypted?

DATA PROTECTION SOLUTIONS

Encryption

- **Best way to secure data, converts data into unreadable form**
- **Office 2007/2010/2013 has encryption feature**
- **Use Vera Crypt www.veracrypt.org**
- **PDF Portfolio**
- **Microsoft Rights Mgt Service (RMS)**
- **PGP Netshare**

SSL

- **Make sure all interactions are done over a secure network (e.g. https)**

Back up your data

businessPractice2012 - Microsoft PowerPoint

Prepare the document for distribution

Properties
View and edit presentation properties, such as Title, Author, and Keywords.

Inspect Document
Check the presentation for hidden metadata or personal information.

Encrypt Document
Increase the security of the presentation by adding encryption.

Restrict Permission
Grant people access while restricting their ability to edit, copy, and print.

Add a Digital Signature
Ensure the integrity of the presentation by adding an invisible digital signature.

Mark as Final
Let readers know the presentation is final and make it read-only.

Run Compatibility Checker
Check for features not supported by earlier versions of PowerPoint.

New, Open, Save, Save As, Print, Prepare, Send, Publish, Close

PowerPoint Options | Exit PowerPoint

DATA PROTECTION SOLUTIONS

ncryption

Best way to secure data, converts data into nreadable form

Office 2007/2010 has encryption feature

Use True Crypt www.truecrypt.org

MS Office

Watch video on our site on how to install nd run True Crypt

SSL

➢Make sure all interactions are done over a secure network (e.g. https)

Back up your data

Click to add notes

Slide 24 of 33 | "New-ITSO" | 75%

Calendar - Microsof... | Interview Notes | 25 Infosec Gurus Ad... | businessPractice2012 | vt owners guide to ... | 1:17 PM

PHYSICAL SECURITY

Don’t assume physical security!!

Key component is location and accessibility of computers

Keep areas locked when necessary and consider restricted access

Laptops and PDAs require additional security measures – especially if those devices contain confidential data

Disable Auto-Logon on any computers

WIRELESS SECURITY

Always use encryption when sending sensitive data

-Make sure website is secure (e.g. https)

Use encryption tool to encrypt files or folders

-Use VeraCrypt to encrypt data being sent

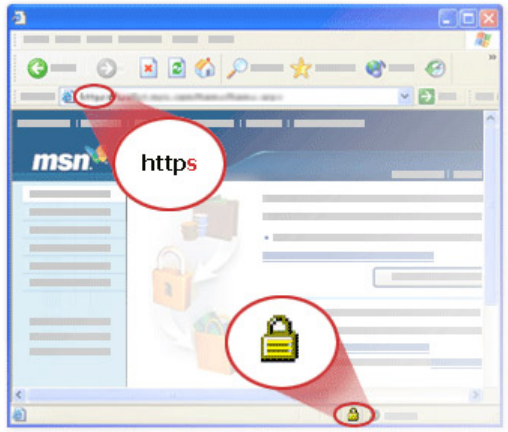
Use secure wireless networks

Make sure connection is the real deal

-Is Mcdonalds1234 the real McDonalds wireless network

USING SECURE WEB SITES

Make sure the website you are using is https and shows a lock in the lower right corner before any sort of transaction



Simply put, you don't want your personal or confidential information broadcast to the world for all to see, especially important on wireless.

SOCIAL NETWORKING

GOOD AND BAD

The good things:

- Keep in touch with colleagues at a distance
- Useful in distance classes
- Find others with your interests or peers in your field

The bad things:

- Can be used to harvest personal information
- Difficult to remove the information when you no longer want it displayed
- Employers are using it for references more frequently

DATA BREACH FRAMEWORK

What to do in the event of a data breach

Need to obtain the following info

- **what sensitive data was on the target?**
- **who attacked the machine, when and how?**
- **Was data exfiltrated outside of your net?**

Have notification templates ready

http://security.vt.edu/downloads/forms/data_exposure/data_expsoure.pdf

WHAT IF IT GETS IN THE WRONG HANDS ?

- **Loss of Intellectual Property**
  - Patents, Copyrights, Royalties
- **Notifications letters (PII)**
  - Identity Protection services for those affected ($15/person/year) paid by the department
- **Image will be damaged**
- **Internal or external investigations**

SUMMARY

Protect data regardless of location

Data Trustees/steward control access to sensitive data

Define data sensitivity levels

Before you protect, you must detect

Use existing protection tools

Have a data breach strategy in place