

OFFICE OF THE ATTORNEY GENERAL PRESENTS

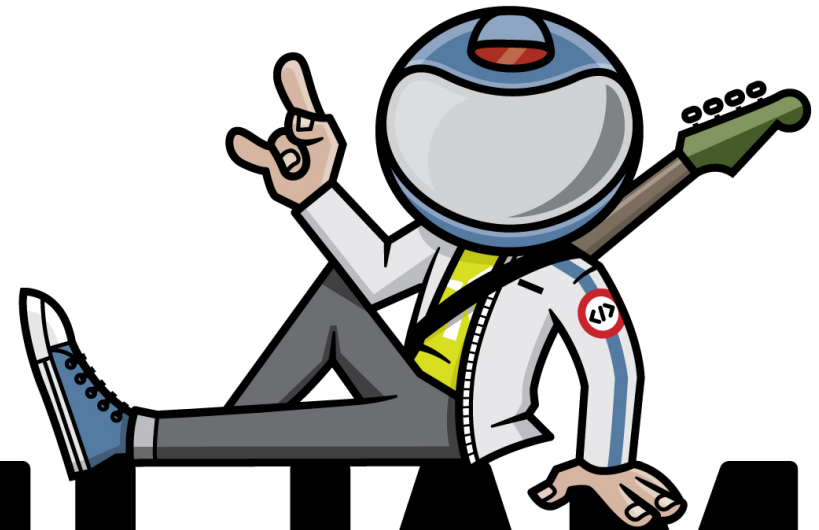
# #WhatTheHack?!



Data security and  
online privacy for  
small businesses

@**TECH JAM**

OCTOBER 20, 10-NOON  
CHAMPLAIN VALLEY EXPO



VERMONT

# TECH JAM

## **Today's presenters:**

Ryan Kriger, CIPP/US

Office of the Vermont Attorney General

Assistant Attorney General, Public Protection Division

Bill Carrigan, CFE

Vermont Department of Financial Regulation

Deputy Commissioner, Securities Division

Investor Education Coordinator

Jonathan Rajewski, MS, CCE, EnCe, CISSP, CFE, TJFC

Champlain College

Founder & Director, the Senator Patrick Leahy Center for Digital Investigation

Associate Professor of Cyber Security and Digital Forensics

Sona Makker, CIPP/US and Claire Gartland

Facebook, Privacy and Public Policy



**Ryan Kriger, CIPP/US**

**Office of the Vermont Attorney General**

**Assistant Attorney General**

**Public Protection Division**



# Data Security for Small Businesses

Ryan Kriger, CIPP/US

Assistant Attorney General, Public Protection Division

October 20, 2017



# Takeaways:

1. Know what laws affect you
2. Train your employees
3. Think data security *before* you get hit
4. Have response plan for *after* you get hit
5. Get Cyber Insurance
6. Vendors/Contractors/Cloud Providers

# Know What Laws You Have To Comply With

- **Consumer Protection Act:** EVERYONE
- **Security Breach Notice Act:** EVERYONE
- **SSN Protection Act:** Do you Collect SSN
- **HIPAA:** Do you do medical work?
- **FERPA:** Do you work with schools/universities?
- **COPPA:** Do you sell to kids under 13?
- **GLB:** Do you work with financial institutions?

# Three Numbers

14

Days: Time to Confidentially Provide Preliminary Notice of Breach to AG

45

Days: Maximum Time to Send Notice to Consumers (It Can Often Be Sooner)

10,000

Dollars: Maximum Civil Penalty Per Violation



**DON'T CLICK  
THE LINK.**



# What Sort of Data Should You Be Protecting?

- Credit Card info
- Social Security Numbers
- Financial Information
- Passwords
- Anything sensitive that someone might not want to fall into the wrong hands



## Have Data Collection Policies:

- Don't collect data you don't need
- Only keep data as long as you need it
- Consider using a 3rd party vendor to handle sensitive data

# Technology Suggestions

## Credit Cards:

- Search your systems to make sure you're not storing data
- Search for key loggers
- Frequent system scans
- Watch your employees
- Consider scanners that encrypt at swipe
- NO web browsing on POS Systems

# Watch Out For Portable Data:

- Cell Phones
- Tablets
- Laptops
- External Hard Drives
- Thumb Drives
- Data In Transit (including E-Mail)
- And Don't Forget Back-up Tapes

# Protect Portable Data:

- Password Protection
- Remote Wipe Capability
- Encryption
- Ask yourself: Should this be in a portable medium?

# I've Had a Data Breach, What Next?

1. Secure Your Data
2. Contact Law Enforcement
3. Contact Cyber Insurance
4. Contact Entities From Which You Obtained the Data
5. Notify the Attorney General's Office Of The Breach
6. Notify Consumers Of The Breach
7. Notify the Credit Reporting Agencies (if more than 1,000 consumers)

# Online Resources

- VT Attorney General Site ([ago.vermont.gov/focus/consumer-info/privacy-and-data-security1.php](http://ago.vermont.gov/focus/consumer-info/privacy-and-data-security1.php))
- OnGuardOnline.gov
- [business.ftc.gov](http://business.ftc.gov)
- IAPP: [www.privacyassociation.org](http://www.privacyassociation.org)



**CYBER INSURANCE**  
**CYBER INSURANCE**  
**CYBER INSURANCE.**





# Questions About Data Breaches?

Contact Us:

**802-828-3171**

**[ago.datasecurity@Vermont.gov](mailto:ago.datasecurity@Vermont.gov)**

Report Breaches:

**[ago.securitybreach@Vermont.gov](mailto:ago.securitybreach@Vermont.gov)**



**Bill Carrigan, CFE**

**Vermont Department of Financial Regulation**

**Deputy Commissioner, Securities Division**

**Investor Education Coordinator**

## DFR Overview

- Department is made up of four Divisions
  - Banking, Insurance, Securities, Captive Ins.
- All Divisions may deal with different aspects of fraudulent activity.
- *The opinions and comments made today are mine and are not the position of the Department.*

# Introduction

- Fraud, in all its forms, costs billions in damage each year.
- Fraud involves taking something from someone else through deception or concealment.
- *Occupational frauds* are those committed in connection with the fraudster's occupation.

# Examples of Occupational Fraud

- Stealing money or inventory
- Claiming overtime for hours not worked
- Filing fraudulent expense reports
- Giving friends or relatives unauthorized discounts on company merchandise or services
- Adding ghost employees to the payroll

# Types of Fraud

*Asset Misappropriation*: schemes in which the employee steals or misuses an organization's assets

- Skimming cash receipts
- Falsifying voids and refunds
- Tampering with company checks
- Overstating expenses

# Types of Fraud

*Corruption:* schemes in which a fraudster wrongfully uses his influence in a business transaction for the purpose of obtaining a benefit for himself or another person

- Conflicts of interest
- Illegal gratuities
- Bribery



# Types of Fraud

*Fraudulent statements:* fraud schemes involving the intentional misreporting of an organization's financial information with the intent to mislead others

- Creating fictitious revenues
- Concealing liabilities or revenues

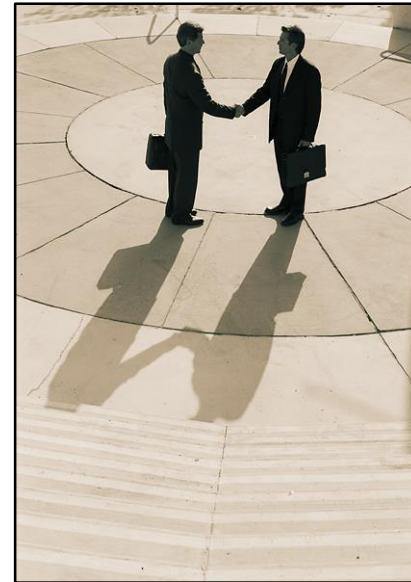


# Common Frauds by Employees

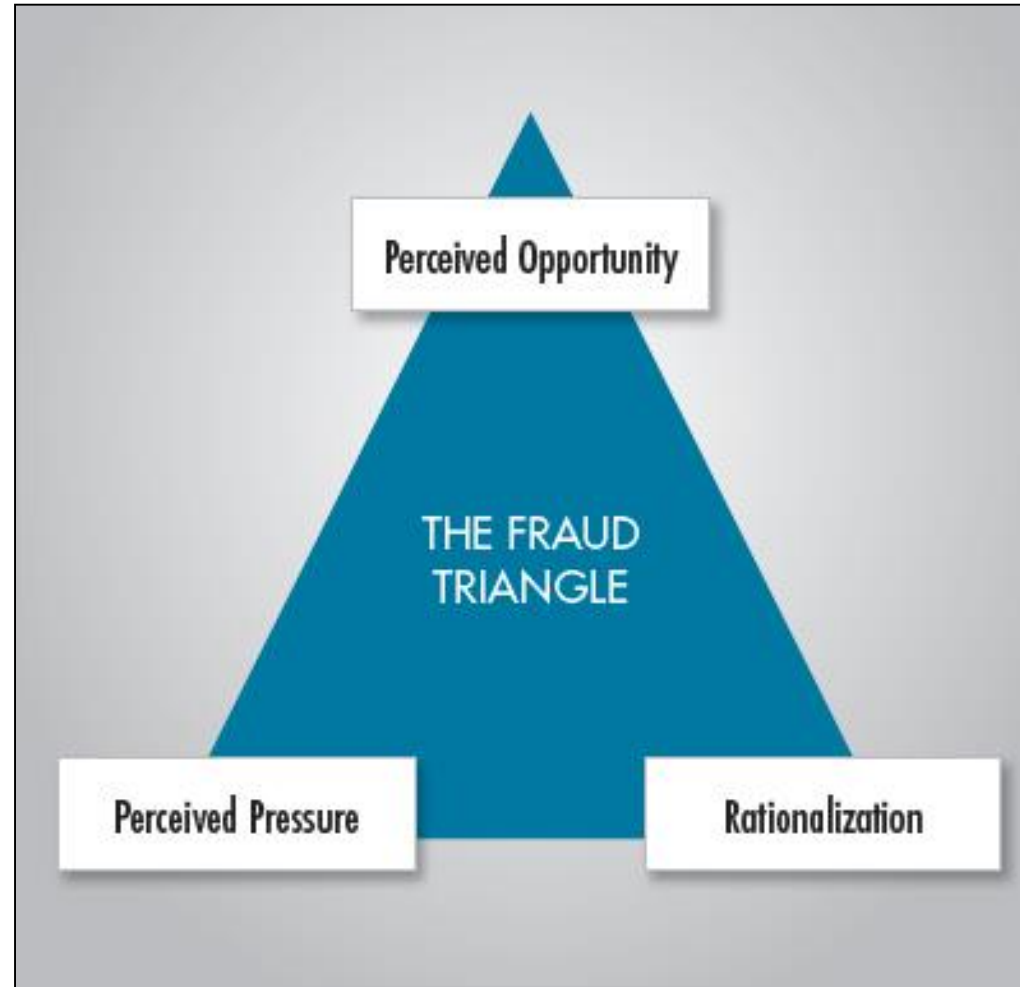
- Stealing incoming cash
- Fraudulent disbursements
  - Check tampering
  - Register disbursement
  - Billing
  - Expense reimbursement
  - Payroll
- Inventory fraud schemes

# Common Frauds by Vendors

- Bid-rigging
- Price-fixing
- Overbilling
- Kickbacks
- Shell companies



# What Causes People to Commit Fraud?



# What Causes People to Commit Fraud?

## *Pressure*

- A gambling or drug habit
- Personal debt or poor credit
- A significant financial loss
- Peer or family pressure to succeed



# What Causes People to Commit Fraud?

## *Opportunity*

- Lack of supervision
- Poor internal controls
- Poor record keeping
- Extreme trust in a single individual
- Lack of disciplinary action for previous frauds

# What Causes People to Commit Fraud?

## ***Rationalization***

- *I was only “borrowing” the money and planned to repay it.*
- *The company won’t even realize this amount is gone; it’s not that much.*
- *My boss does it all the time.*

# What Causes People to Commit Fraud?

## ***Rationalization***

- *I've been working with the company for 15 years. They owe it to me.*
- *I'll stop once I pay off my debts.*
- *I deserved this after the way the company has treated me.*

# How Fraud Affects You and Your Organization

- Fewer pay increases
- Increased layoffs
- Greater pressure to increase sales and revenue
- Decreases in employee benefits
- Low employee morale
- Negative publicity for the company



# Red Flags of Fraud

- Living beyond means
- Financial difficulties
- Serious addiction to drugs, alcohol, or gambling



# Other Warning Signs of Fraud

- An unwillingness to share duties
- A refusal to take vacations
- A close personal relationship with vendors or customers
- Complaints about low pay
- Family problems
- Excessive pressure within the company
- Rule breakers

# What to Do if You Suspect Fraud

- Be aware of warning signs
- Report irregularities, specifically:
  - If someone you work with asks you to do something that is illegal or unethical
  - If you suspect that someone— regardless of rank or position—is committing fraud or abuse

# How to Report Suspected Fraud

- Hotlines or other anonymous reporting mechanism
- Anonymous letter to company official
- Share your concern with company's internal auditors or anti-fraud specialists

# Conclusion

- Everyone in an organization is responsible for fighting fraud.
- Be alert to potential fraud.
- Report any suspicions to your organization.





**Jonathan Rajewski, MS, CCE, EnCe, CISSP, CFE, TJFC**

**Champlain College  
Associate Professor of Cyber Security and Digital  
Forensics**

**Founder & Director  
Senator Patrick Leahy Center for Digital Investigation**



**LCDi** | Leahy Center for Digital Investigation

*"Behind this glass is incredible talent and this country in general and the FBI in particular needs those folks,"*

*-FBI Director James Comey*







# Do you think your data is safe?

## What

databases  
email  
spreadsheets  
documents  
pictures  
videos

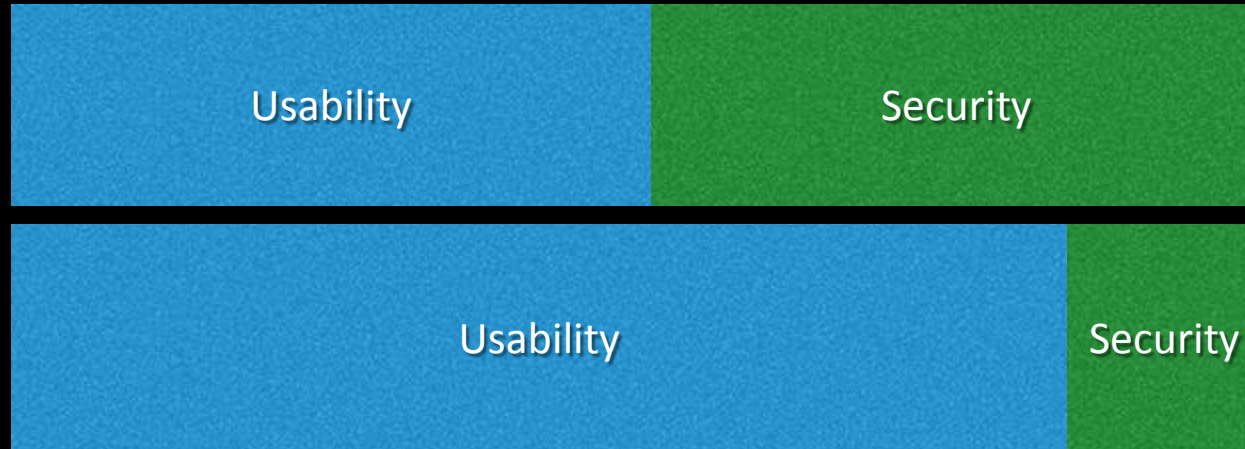
## Where

laptops / tablets  
computers  
removable  
devices  
servers  
cloud

## Specifically

Personal Identifiable Information  
Protected Health Information  
Private / Sensitive Information

# Why isn't the data on our networks secure?



# Total security is a myth



# Ask your IT staff two questions...

When was the last time they experienced  
a data breach?

Are they currently breached?

Executive  
Management

Legal

Human  
Resources

Information  
Technology

Our job is to  
manage

Our job is to  
shift liability

Our job is to  
avoid trouble

Our job is to  
make it work

Security is  
both a legal  
and IT problem

Security is a  
technical  
problem

Security is  
trouble

Employee  
behavior is not  
our problem

## Effective/Clear/Accountable Policy

Executive  
Management

Legal

Human  
Resources

Information  
Technology

Our job is to  
manage

Our job is to  
shift liability

Our job is to  
avoid trouble

Our job is to  
make it work

Security is  
both a legal  
and IT problem

Security is a  
technical  
problem

Security is  
trouble

Employee  
behavior is not  
our problem

# Demystify cyber security



**Administration**

[Home](#) > [Administration](#) > [Local Municipalities at Greater Risk to be "Hacked"](#)

Posted on: July 26, 2017 0 [Like 0](#) [Twitter](#) [LinkedIn](#) 0 [+](#) 0 [Email](#)

## Local Municipalities at Greater Risk to be "Hacked"

Limited funding coupled with infrastructure capabilities have made public works and municipalities a new favorite for hackers.



Hacking has been on the mind of many Americans after reported election interference by the Russian government. In fact a recent Gallup poll noted that seven out of 10 Americans worry about hacking, placing it atop the list of crimes that Americans worry about most.

But instead of major national breaches that target top companies and government agencies, what experts say should be most alarming are networks at the local level. Cybersecurity at the local level can be summed up in a single word: "deficient." That

is according to Don Norris, a professor at the University of Maryland, Baltimore County.



# Deloitte hit by cyber-attack revealing clients' secret emails

**Exclusive:** hackers may have accessed usernames, passwords and personal details of top accountancy firm's blue-chip clients



<  
12,022

Nick Hopkins

Monday 25 September 2017 08:00 EDT



Deloitte provides auditing, tax consultancy and cybersecurity advice to banks, multinational companies and government agencies. Photograph: Alamy Stock Photo

One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients, the Guardian can reveal.

OPINION | COMMENTARY

## On Behalf of Equifax, I'm Sorry

A new free service will let consumers lock or unlock access to their credit data any time they like.

*By Paulino do Rego Barros Jr.*

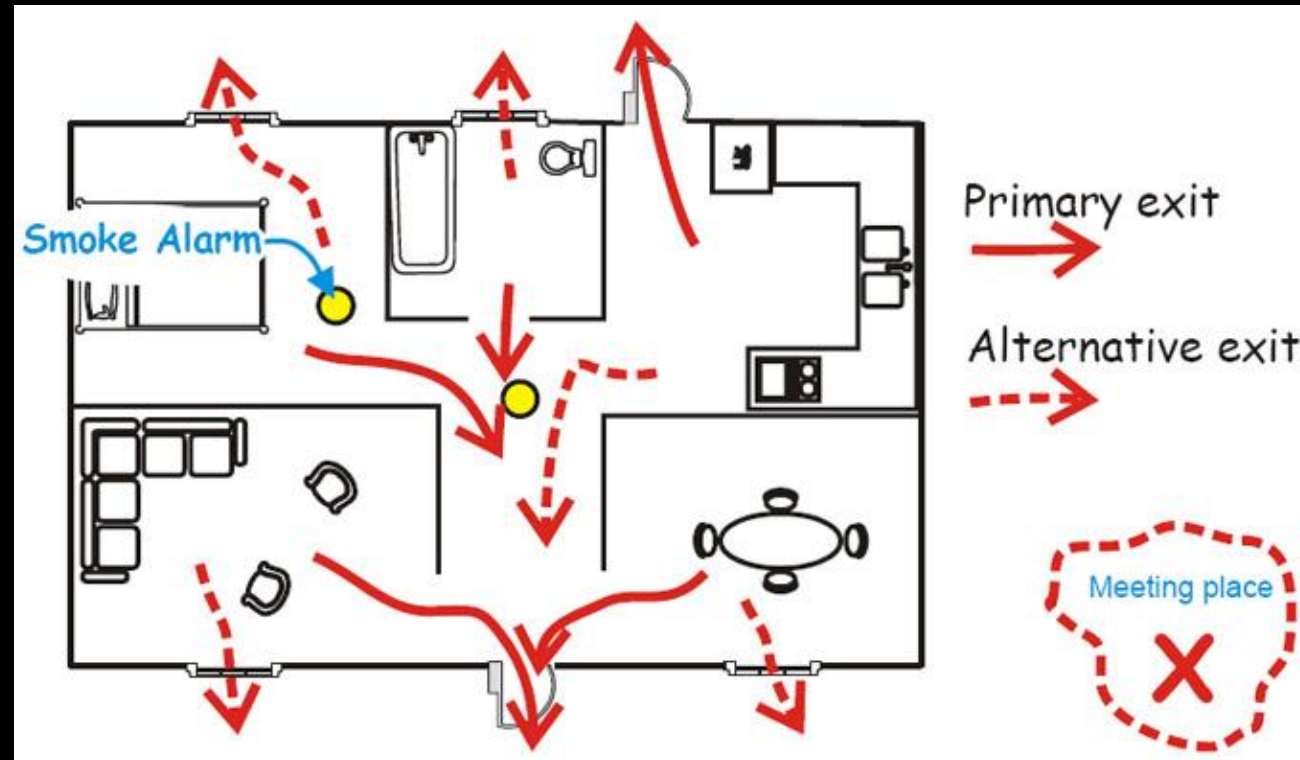
Sept. 27, 2017 5:20 p.m. ET

On behalf of Equifax, I want to express my sincere and total apology to every consumer affected by our recent data breach. People across the country and around the world, including our friends and family members, put their trust in our company. We didn't live up to expectations.

We were hacked. That's the simple fact. But we compounded the problem with insufficient support for consumers. Our website did not function as it should have, and our call center couldn't manage the volume of calls we received. Answers to key...

So how do we reduce the risk to a reasonable level?

It's not if you're going to have a cyber related event, it's when



# Part of the plan should be insurance...

## Cyber insurance is changing the way we look at risk

Posted Jun 13, 2016 by [Yoav Leitersdorf](#), [Ofar Schreiber](#), [Iren Reznikov](#)

### Breaking down a cyber insurance policy

Most cyber policies currently on the market offer a combination of two types of insurance coverage:

- First-party coverage: covers direct losses to the organization.
- Third-party coverage: protects against claims against the organization by third parties, such as customers or partners.

Besides financial coverage, insurers also provide risk management and post-breach services, including loss-prevention measures and remediation tools.

# Part of the plan should be insurance...

## 2016 Breach costs - \$290 - \$15MM

Crisis services costs (forensics, notification, credit monitoring and legal counsel),  
Legal damages (defense and settlement),  
Business interruption costs  
Fines (PCI and regulatory) by the type of data exposed

2016 Typical breach cost \$5,822 - 1.6MM 80% - 10th-90th percentile

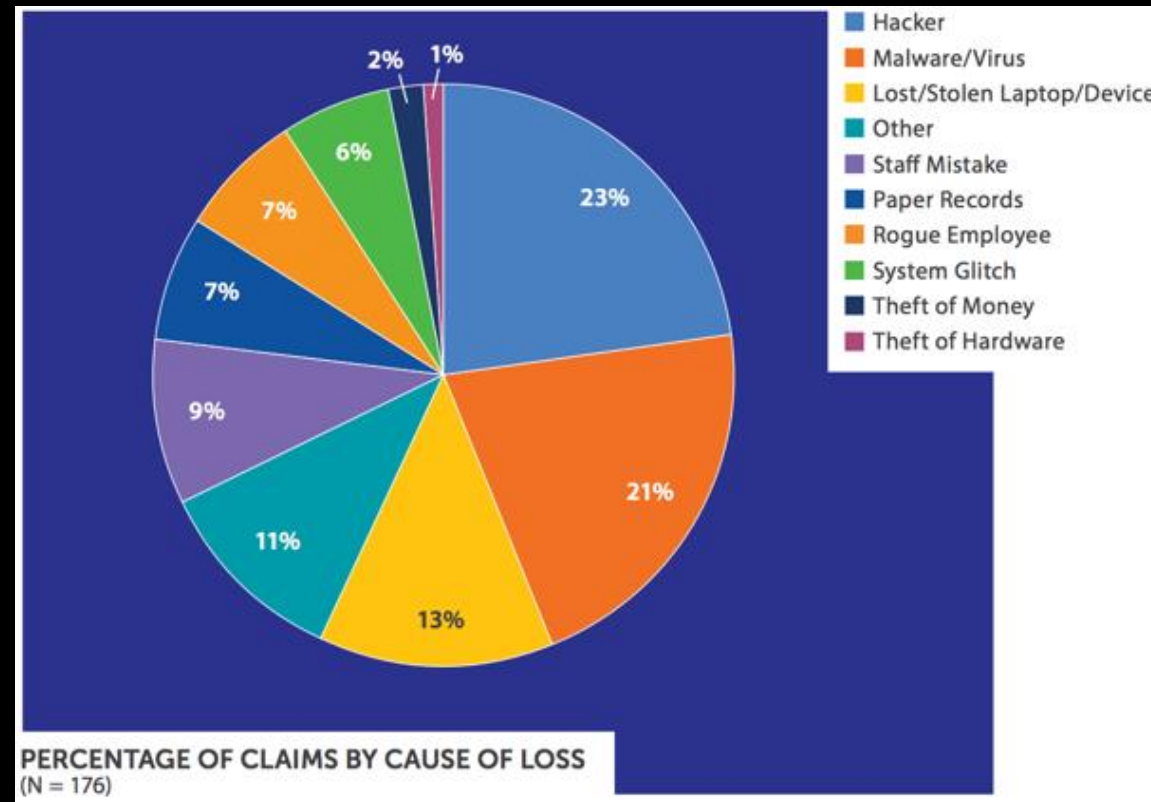
2016 Average Claim \$495,000

# Part of the plan should be insurance...

CRISIS SERVICE COSTS						
Service	Claims with Costs	Total	Min	Median	Mean	Max
Forensics	106	18,983,603	1,234	35,450	179,091	2,456,000
Notification	53	8,942,659	58	5,000	168,729	2,000,000
Credit/ID Monitoring	57	15,990,149	298	12,198	280,529	2,900,000
Legal Guidance/Breach Coach*	109	11,012,155	290	28,394	101,029	2,500,000
Public Relations/Other	34	1,843,399	15	6,839	54,218	1,065,000

N=176

# Part of the plan should be insurance...



It's not just about shifting risk...



# Practical Takeaways





## Workplace Health Promotion

### Home

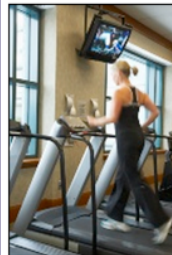
- Making a Business Case
- Workplace Health Model
- Assessment
- Planning/Workplace Governance
- Health Topics Addressed
- Implementation
- ▶ **Physical Activity**
- Evaluation
- Help/FAQs
- Glossary
- References
- Links to Organizations
- Partners
- Site Map

[Home](#) > [Implementation](#)

[Recommend](#) [Tweet](#) 2 [Share](#)

[Email page link](#)  
[Print page](#)

## Physical Activity



Once [assessment](#) and [planning](#) have been completed, including analysis of the collected data, the next step is implementing the [strategies and interventions](#) that will comprise the workplace health program. The intervention descriptions below provide the [public health evidence base](#) for each intervention, details on designing physical activity interventions, and links to examples and resources.

**Before implementing any interventions, the evaluation plan should also be developed.** Potential baseline, process, health outcome, and organizational change measures for these programs are listed under [evaluation of physical activity programs](#).

Regular [physical activity](#) is one of the most effective disease prevention behaviors. Physical activity programs:

- Reduce feelings of [depression](#)
- Improve stamina and strength
- Reduce [obesity](#) and particularly when combined with diet
- Reduce risks of cardiovascular disease (e.g., high [blood pressure](#) and [cholesterol](#), stroke, and [type 2 diabetes](#))

Physical activity programs can range from simple to extensive, with varying implementation costs. The primary purposes of workplace interventions are to encourage employee education and physical activity.

### On This Page

- [Health-related programs for physical activity](#)
- [Health-related policies for physical activity](#)
- [Health benefits for physical activity](#)
- [Environmental support for physical activity](#)
- [Tools and resources](#)

### Contact Us:

Division of Population Health/Workplace Health Promotion  
 Centers for Disease Control and Prevention  
 4770 Buford Highway, Northeast, Mailstop K-45  
 Atlanta, GA 30341  
 800-CDC-INFO (800-232-4636)  
 TTY: (888) 232-6348  
[Contact CDC-INFO](#)

[Home](#) > [How It Works](#)

## How It Works

See what the Blue365 lifestyle has to offer. Have 45 seconds to spare? Watch this short video to learn how Blue365 can help you treat your mind and body well – one healthy choice at a time.



### Two Ways to Save

The health and wellness deals, designed just for you, will help you save on all you need to keep fit. Even better? You'll have access to two types of good-for-you deals: standing discounts (which you can redeem anytime you like) and exclusive, limited-time offers designed for living well – right in the moment.

## Frequently Asked Questions

Do you have a question about...

[Blue Cross and Blue Shield Companies?](#)

[Blue365?](#)

[Blue365 Vendors?](#)

[Browsing, buying or redeeming a Blue365  
Featured Deal or Ongoing Deal?](#)

[Problems redeeming a Blue365 Featured Deal  
or Ongoing Deal?](#)

[Blue365 Rewards?](#)

[Sharing information on Blue365?](#)

[Anything Else?](#)

[View All FAQs](#)

## Feature Your Business

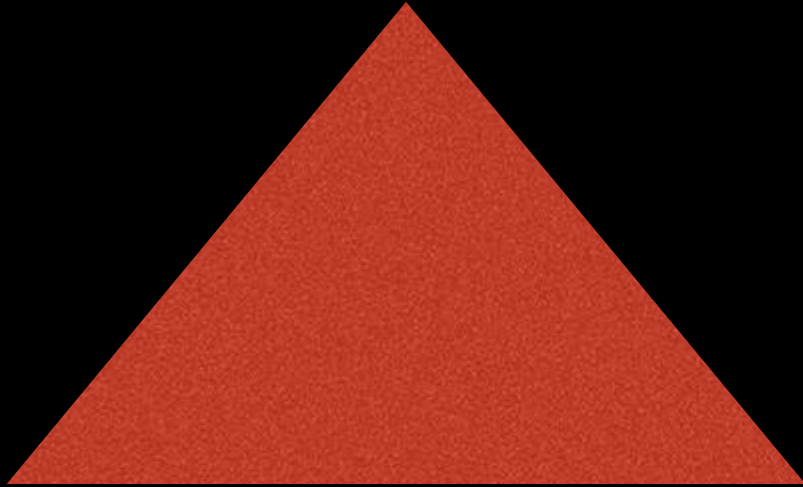


### Does your business have great deals for the Blue365 community?

[Click here](#) to find out how to join the good-health movement.

Being proactive is smart

People



Process

Tools

Where are your risks?  
Determine where you need help  
Budget accordingly

Do you have mandatory trainings?

Stop Drop and Roll

Look both ways before crossing

STOP THINK CONNECT™

PLEASE use a separate passphrase for work and compartmentalize accordingly





# Use Multifactor Authentication



Google Authenticator

Enter this verification code if prompted during account sign-in:

Google  
**581046**  
jtrajewski@gmail.com

Google  
**561551**  
rajewski@champlain.edu


Dropbox  
**254943**  
rajewski@champlain.edu

Dropbox  
**914885**  
jtrajewski@gmail.com

Google

Google

### 2-Step Verification

 Enter the verification code generated by your mobile application.

Enter code


**Verify**

Remember this computer for 30 days.

[Problems with your code?](#)

[create an account](#)

One Google Account for everything Google



# Google's strongest security for those who need it most

The Advanced Protection Program safeguards the personal Google Accounts of those most at risk of targeted attacks—like journalists, business leaders, and political campaign teams.



## The strongest defense against phishing

Phishing is one of the most common techniques hackers use to gain access to your account or personal information. For example, phishing emails or fake sign-in pages could trick you into revealing critical information, like your password.

## You'll need 2 Security Keys to turn on Advanced Protection

Already have Bluetooth and USB Security Keys? [You can skip this step.](#)

- 1 Buy 1 Bluetooth key that'll work on your phone, tablet & computer (with a cable)



Main key (Bluetooth)  
Feitian MultiPass FIDO Security Key

[BUY FROM AMAZON](#)

- 2 Buy 1 USB key for computer use



Backup key (USB)  
Yubico FIDO U2F Security Key

[BUY FROM AMAZON](#)

[Having trouble ordering Security Keys?](#)

“CEO fraud,” or “business email compromise.”

\_HELP\_INSTRUCTION - Notepad

File Edit Format View Help

!! INFORMATIONS!!

All your files are encrypted with RSA2048 and AES128 ciphers.  
More information about the RSA and AES can be found here:  
URL:1 [https://en.wikipedia.org/wiki/RSA\\_numbers](https://en.wikipedia.org/wiki/RSA_numbers)  
URL:2 [http://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

Decrypting your files is only possible with  
the private key and decrypts programs, which is on our secret server.

Follow these steps:

1. Download and install Tor\_Browsers: <http://torproject.org/download/download-easy.html>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the address bar: [http://\[REDACTED\].onion](http://[REDACTED].onion)
4. Follow the instructions on the site.

!! Your DECRYPT-ID: [REDACTED] !!

# How to deal with ransomware

- Don't click or open attachments/links that look suspicious
- Be careful on social media - videos are not really videos etc...
- Backup your files! (cloud?) & TEST BACKUPS
- Call for help!

# How many of you have ever connected to...



# So what can you do?

The screenshot shows the F-Secure Freedom website with a navigation bar at the top containing links for 'All Devices', 'Desktops & Laptops', 'Mobiles & Tablets', 'Tips & Tricks', and 'Support', along with a 'My F-Secure' user profile icon. The main content area is divided into four quadrants, each featuring a purple icon, a title, a brief description, and a 'How does this work?' button.

- PRIVATE AND UNTRACKABLE**: Represented by an eye icon with a slash through it. Description: 'Say no to snoops and annoying advertisers tracking you. Freedom is privacy, anonymity and digital freedom.'
- REMOVE GEO-RESTRICTIONS**: Represented by a location pin icon. Description: 'Change your virtual location to access blocked services while adding an extra layer of privacy to your surfing.'
- WI-FI SECURITY**: Represented by a Wi-Fi signal icon. Description: 'Freedom shields you on public Wi-Fi – your data is protected even in vulnerable unsecured hotspots.'
- SAFE SURFING**: Represented by a globe icon. Description: 'With the push of a button, Freedom gives you your own private network, blocking bad apps and harmful sites.'

- Use your phone as a wifi hotspot
- Ensure you trust which wifi you are connecting to
- Use a Virtual Private Network



# Antivirus

It can be compared to the  
flu shot....

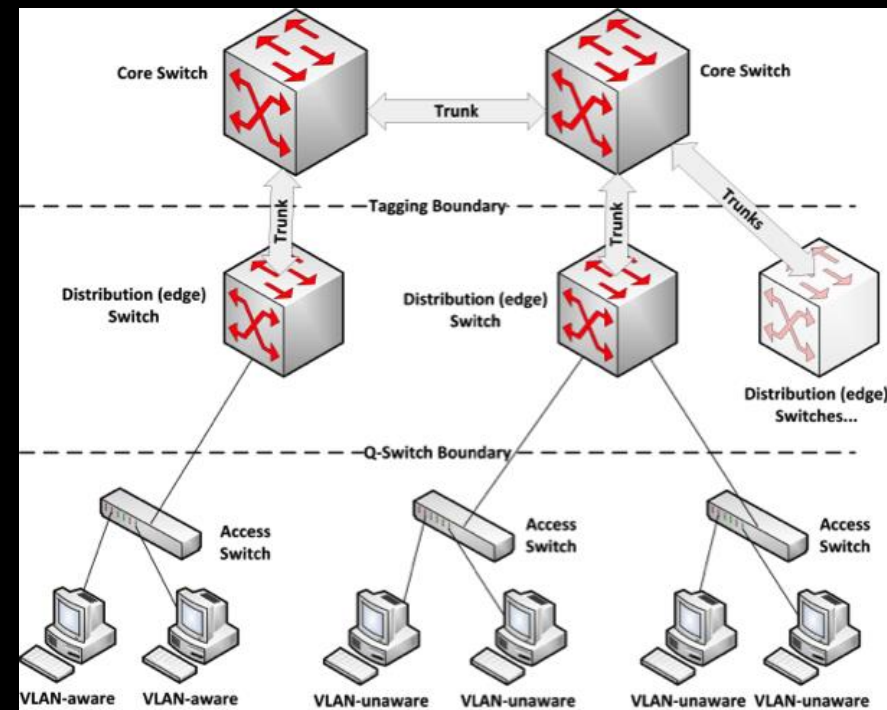


# General Cyber Security Tips IT professionals

A current asset list and network map

Data classification - where do you have the crown jewels

# General Cyber Security Tips IT professionals



# General Cyber Security Tips IT professionals

1 **echo**

Always ready, connected, and fast. Just ask.

\$99<sup>99</sup> [Learn more](#)



3 **echo spot**

Stylish, compact Echo with a screen

\$129<sup>99</sup> [Learn more](#)



5 **echo connect**

Turns your Echo into a voice-controlled speakerphone

\$34<sup>99</sup> [Learn more](#)



2 **echo plus**

With built-in smart home hub

\$149<sup>99</sup> [Learn more](#)



4 **fire tv**

With 4K Ultra HD and Alexa Voice Remote

\$69<sup>99</sup> [Learn more](#)



6 **echo buttons**

Bringing even more fun and play into your home

[Learn more](#)



Introducing  
**echo show**  
Now Alexa can show you things



**echo look**



Love your look. Every day.

# General Cyber Security Tips IT professionals

Enable logging on internal and external systems

**NOTE:** You have to first turn on audit logging before you can run an audit log search. If the **Start recording user and admin activity** link is displayed, click it to turn on auditing. If you don't see this link, auditing has already been turned on for your organization.

# General Cyber Security Tips IT professionals

Collect data that's important to hunt for evil

System Event Logs	DHCP Logs
Proxy Logs	SMTP/Mail Logs
Firewall Logs	Remote Desktop/VPN Logs
Intrusion Detection Logs	Active Directory Logs
Anti-Virus Logs	Application Logs
Flow Data	ALL OF THE LOGS?

Data retention?    Do you have time?    Do you know what to look for?

Search (e.g. status:200 AND extension:PHP)

Uses lucene query syntax 🔍

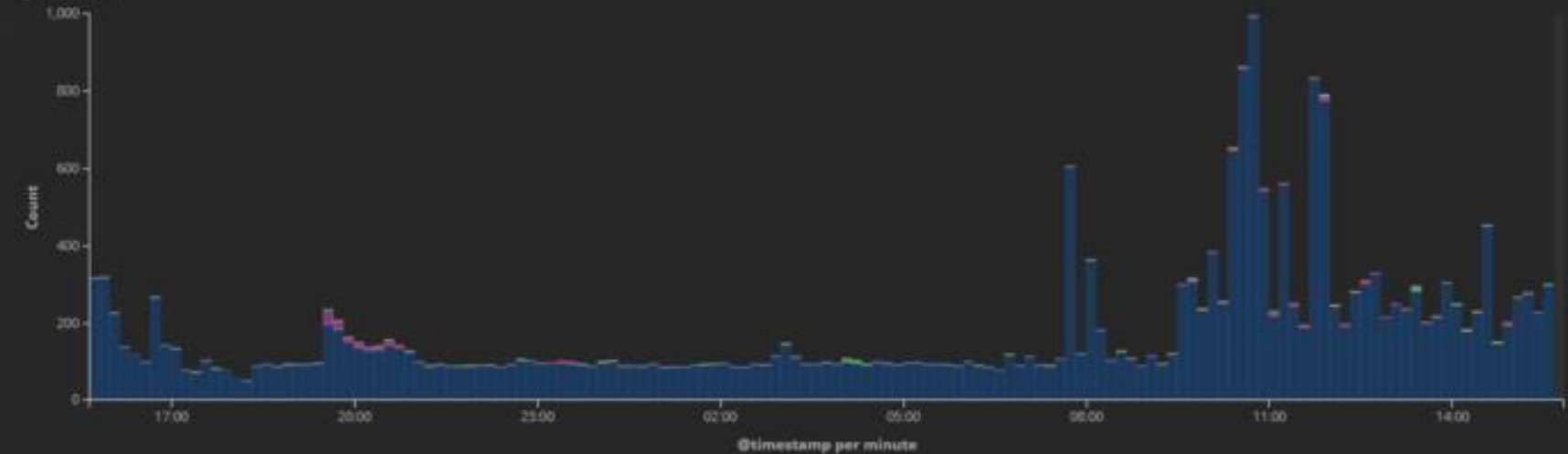
- Discover
- Visualize
- Dashboard
- Timeline
- Dev Tools
- Management

Add a filter +

Total pfSense Logs

Count  
**270,668**  
Count

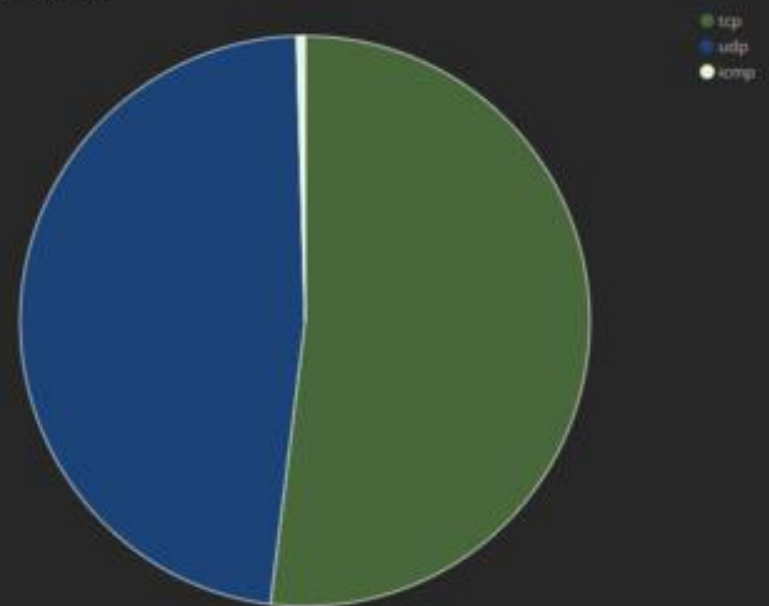
pfSense IPs



SOC - pfSense Geo Map



pfSense Protocols



Search: (e.g. status:200 AND extension:PHP)

Uses lucene query syntax

- Discover
- Visualize
- Dashboard
- Timeline
- Dev Tools
- Management

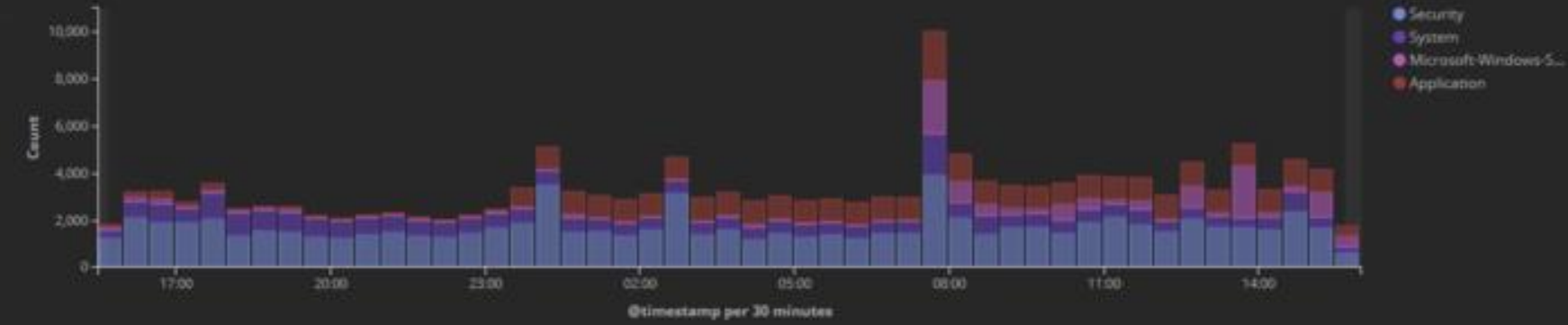
Add a filter

### Winlog Events Counter

# 161,912

Events

### Number of Events Over Time By Event Log 2



### Sources 2



### Top Event IDs 2

event_id: Descending	Count
4,624	37,563
4,634	35,175
1,001	18,811
7,031	14,125
7,040	9,604

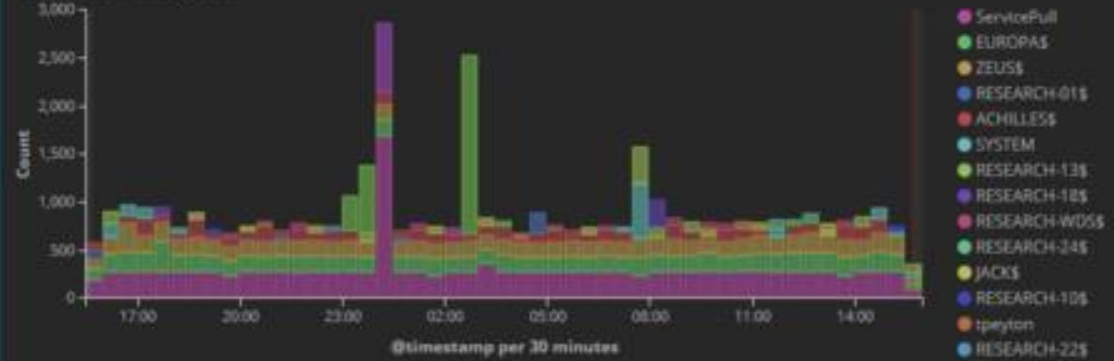
Export: Raw Formatted

### Logs Messages By Host

host.keyword: Descending	Count
Europa	52,725
research-07	43,146
Zeus	29,908
RESEARCH-31	6,602
ACHILLES	4,830
RESEARCH-24	4,665

Export: Raw Formatted

### Events Over Time by User



### User Logins [By: MG]

Time	event_data.TargetUserName	event_data.LogonType	event_data.WorkstationName
October 18th 2017, 15:37:3	ANONYMOUS LOGON	3	-
October 18th 2017, 15:37:3	LOCAL SERVICE	5	-
October 18th 2017, 15:37:3	NETWORK SERVICE	5	-
October 18th 2017, 15:31:2	jnicastro	3	-
October 18th 2017, 15:29:2	asimon	3	-

1-50 of 756



# General Cyber Security Tips IT professionals

Know when it's appropriate to call for help with security/response

Have an expert on retainer

Backups

Conduct them but also test them

Explore regular penetration testing to test your security controls



**Sona Makker, CIPP/US**

**Claire Gartland**

**Facebook, Privacy and Public Policy**

**facebook**

# Privacy Best Practices

**Claire Gartland & Sona Makker**

Facebook Privacy and Public Policy Team

**PRIVACY** *it's good for business*

**knowledge**

**control**

**security**

# 5 Practical Tips for Getting Privacy Right

**#1**

**Designate a "Privacy Advocate"**



**#2**

**Conduct a Data Audit**

understand the

*Who? What?*

*When? Where?*

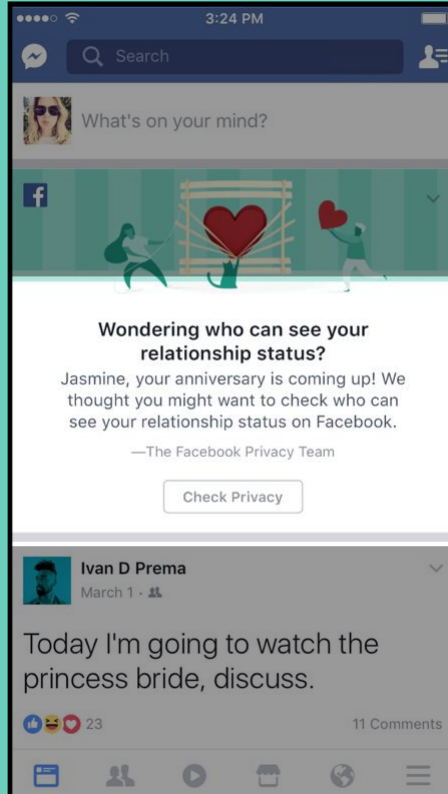
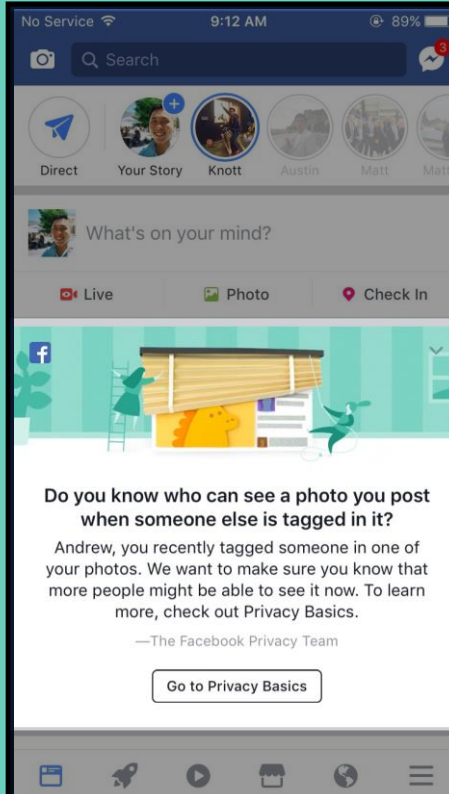
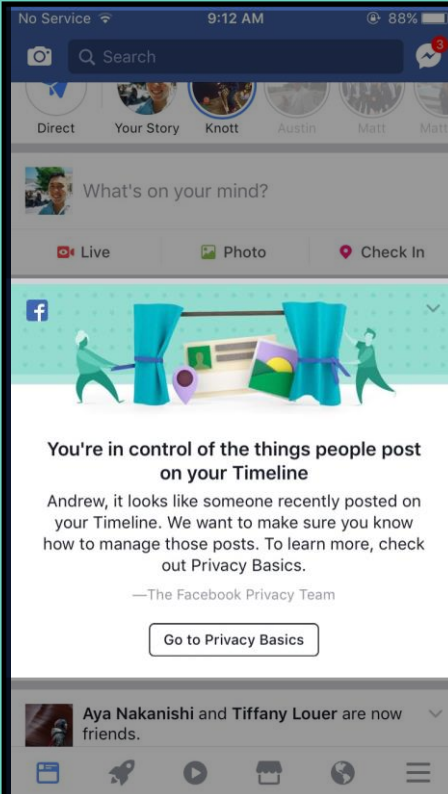
*Why? How?*

of your data practices

**#3**

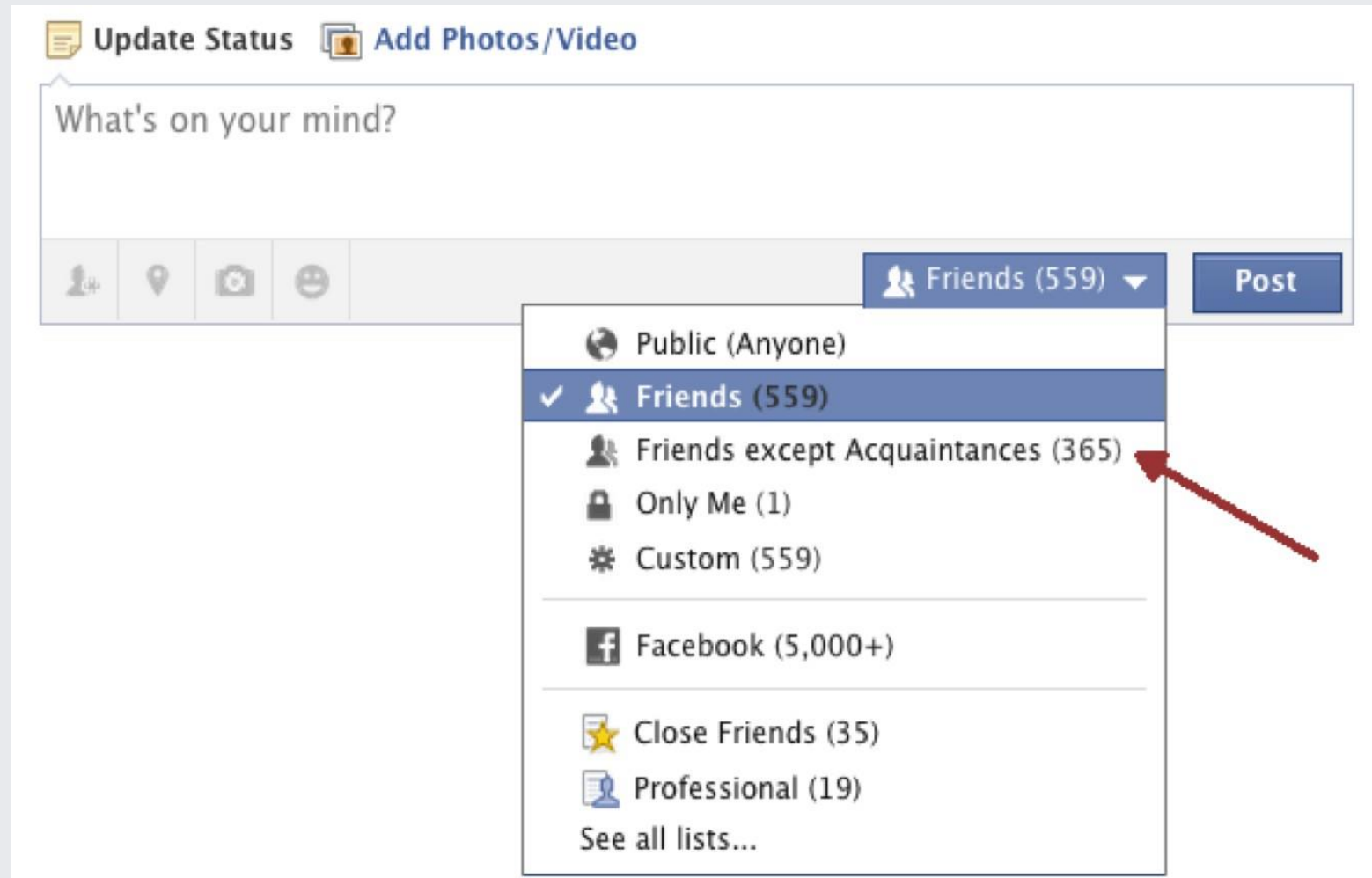
**Build Trust Through  
Transparency**

give people the **right information** at the  
**right time** to make the **choices that are**  
**right for them**



# Avoiding surprises

Make sure people understand the audience they're posting to.



**#4**

**Protect What You Collect**

put users in control

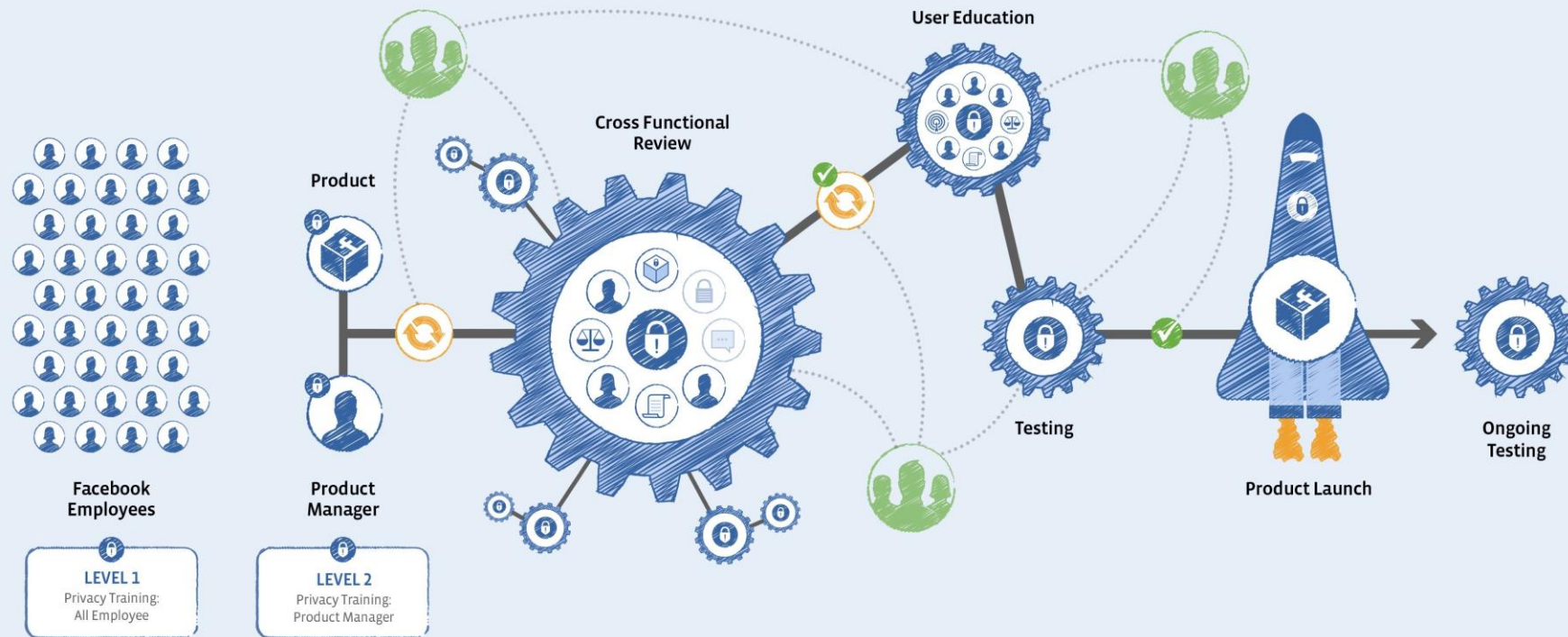
respect expectations

be proactive, not reactive

**Privacy by Design**



facebook | Privacy by Design

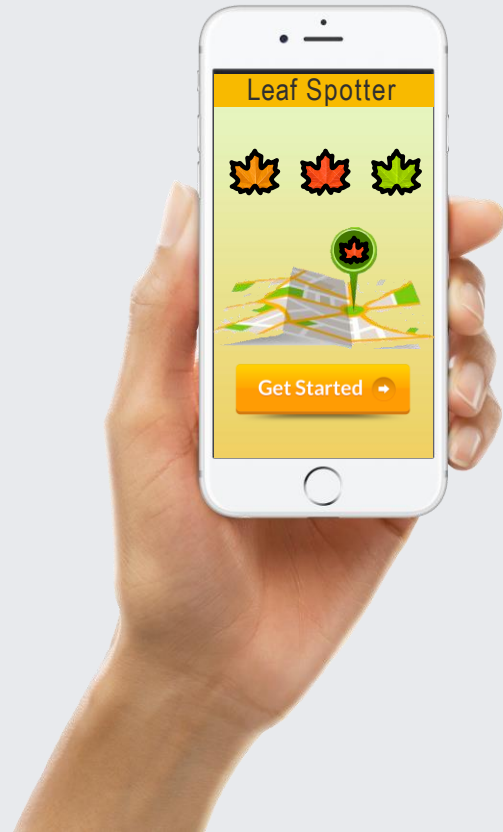


**#5**

**Create a Culture of Privacy**

# Privacy by Design in Practice

## The scenario

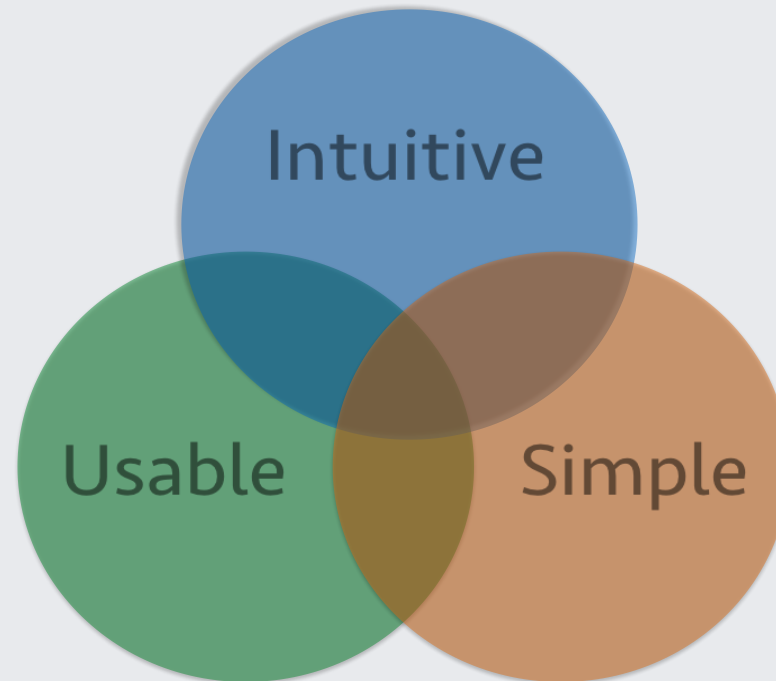


Your company is developing "Leaf Spotter"—a mobile app to crowdsource leaf peeping locations

# Your Task

Design the privacy interface for Leaf Spotter

*Introduce users to features in a way that's usable, intuitive, and simple*



# Considerations

*who are your users?*

*what data do you collect?*

*what do people expect?*



*be transparent.*

*avoid surprises.*

*give people control.*

# Leaf Spotter Data Flow

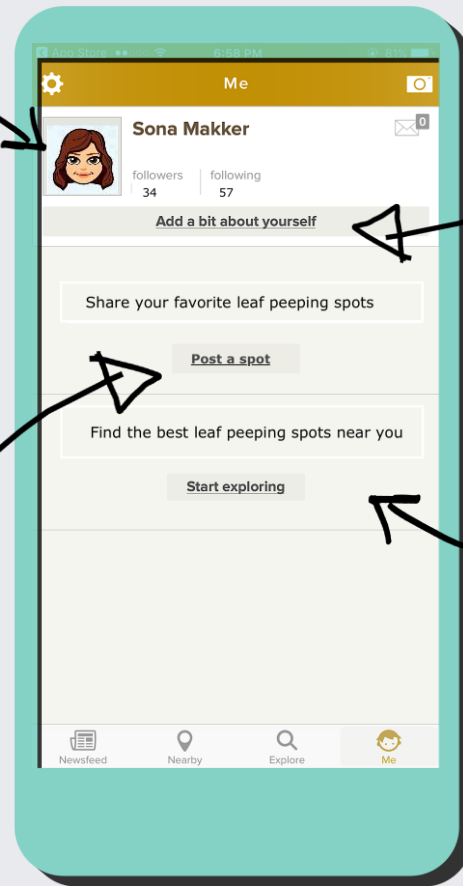
## privacy considerations

*is this public on Leaf Spotter?*

*who can see my bio?*

*who can see my posts?*

*does this use my location?*



# Discussion

1. What were some of the challenges?
2. How can you implement privacy best practices to build trust for your business?





**Thank you!**

OFFICE OF THE ATTORNEY GENERAL PRESENTS

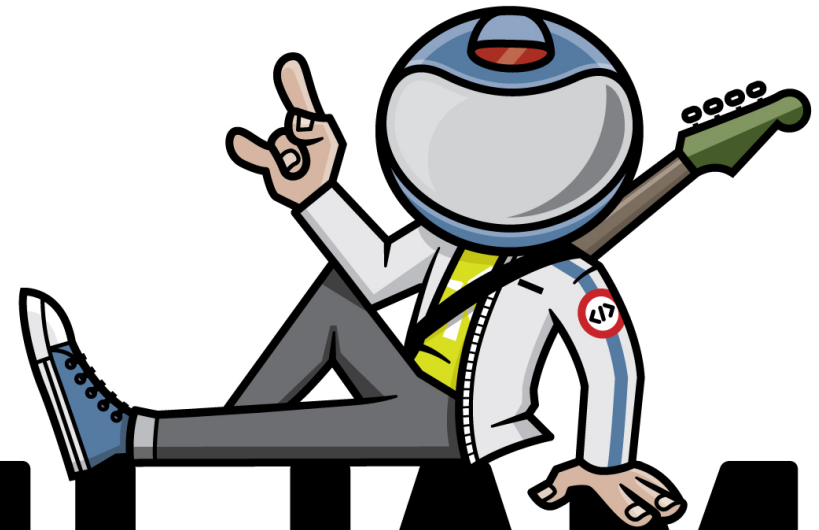
# #WhatTheHack?!



Data security and  
online privacy for  
small businesses

@**TECH JAM**

OCTOBER 20, 10-NOON  
CHAMPLAIN VALLEY EXPO



VERMONT

# TECH JAM