October is scary not just because of Halloween

Dr. Ray Klump
Chair and Professor, Computer & Mathematical Sciences
Director, Master of Science in Information Security
National Cyber Security Awareness Month (NCSAM)

- Annual campaign to raise awareness about cyber security
- Educate public and private sector through events that increase awareness
Each week of NCASM has a theme.
October 3 – 7:

October 10 – 14:

Cyber from the Break Room to the Board Room
October 17 – 21:

Recognizing and Combating Cybercrime
October 24 – 28:

Our Continuously Connected Lives: What’s Your ‘App’-titude?
October 31

Building Resilience in Critical Infrastructure
Why do we need a month for cyber security awareness?
The problem is bigger now than ever.
Why do hackers do this?
Successful hacks raise a lot of money

- $11 per birthdate-name-address
- $20 per health insurance record
- $30 per SSN
- $300 per bank account number
- $1,200 per full identity kit
Successful attacks cause tremendous loss to an organization.

- Average cost of breach: $674K
- Average cost of a healthcare breach: $1.3 million
- Median per-record cost of losing a record: $13
- Average # of records lost: 3.2 million
Most popular causes of attacks

- employee errors
- privilege misuse
- physical theft / loss
- denial of service
- crimeware
- web app attacks
- POS intrusions
- cyber espionage
- payment card skimmers
All together ...

- 31% of cyber loss caused by hackers
- 14% by malware
- 11% by human error
Who’s the target?
Organizations of all shapes and sizes face cyber challenges

- In 2015, 60% of attacks were targeted toward small and medium-sized businesses (SMBs)
- 1 in 2 businesses surveyed in 2014 reported being victim of cyber attack
- 3 out of 4 spear-phishing attacks in August 2015 targeted small businesses with 250 employees or less.
- 60% of SMB cybercrime victims go out of business within 6 months of an attack.
To cope, you need to ...

- Recognize that there is a problem
- Break down the problem
- Acquire the expertise
  - *Currently more than 200,000 cyber jobs are unfilled*
- Acquire the resources to carry out your plan
  - *60% see buy-in as the number one obstacle*
  - *Need to make the case*
- Counteract inertia
Phishing is one of the biggest threats

- We click on duplicitous emails
- Anti-phishing software is getting more popular
And you need to encrypt ... everywhere

- Data that needs to remain secret must be encrypted
- Encrypt data at rest and in transit
- Encrypt on all devices where the data resides
And you need to require more than just a password

- Multifactor authentication is very important today
As if this weren’t enough, critical infrastructures are increasingly at risk.
Today’s Power System
Smart Grid in the Home

How much will you save?
Data in Your Home
Data Everywhere
Where Security Fits In
Challenges

Confidentiality
Integrity
Authentication
Availability
Collection
Storage
Interpretation
Real Consequences
Overload results
The need to work together
So, cyber insecurity wreaks havoc on both small and large scales.
But, cyber security starts with us.
Stop. Think. Connect.

- National public awareness campaign aimed at
  - *Increasing our understanding of cyber threats*
  - *Empowering the American public to be safer and more secure online*
Stop. Think. Connect.

- Cyber security is a shared responsibility.
- Advocates simple steps makes the Internet safer for everyone.
- Provides lots of resources for a variety of Internet users.
- https://www.dhs.gov/stophinkconnect-toolkit
For example:
Smartphone security checklist

- https://www.fcc.gov/smartphone-security
Another example: Social Media

- Telling stats:
  - 64% of teens make their tweets public
  - 19% of teens have posted something they regret
  - Only 18% of adults are comfortable with what their friends post about them online
Beware of what you post online

- Don’t post things that could be used to steal your identity (e.g. your birthday)
- Don’t post anything you wouldn’t want a future employer to see
- Don’t post your location
- Remember that there is no DELETE button on the Internet
Beware of public wifi

- Be careful when you connect
- Avoid conducting sensitive activities
- Use your mobile network connection instead
  - Or use a VPN
Be cautious even when you’re not using a “computer”
Internet of things

- Non-traditional computing devices provide computing services to us
  - *Often collaborating with other such devices*
- Communicate over wifi
- These share information about us
- Systems you don’t usually think of as computers are
  - *Your car*
  - *Your appliances*
- By 2019: 20 billion to 40 billion connected devices
- They must be kept constantly patched
Examples
Who are interested in these devices?

- Criminals
- Law enforcement
- Device manufacturers
Free and open-source can capture the data from these devices

- Wireshark
- FATXplorer
- FTK Imager
- The Sleuth Kit
- Rooting software
- Coolgear USB 3.0 Multifunctional Commutator
Nest

- Reveals a regular traffic pattern when the house is unoccupied
Amazon Echo

- Voice requests
- When voice requests were issued
Xbox – Data saved under gamer id

<table>
<thead>
<tr>
<th>Hex</th>
<th>Strings</th>
<th>Metadata</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>m9k8!</td>
<td>!<del>!Q</del></td>
<td>&amp;USBXML</td>
<td>PlayerProfile uint64 value 6900357706c1056007 nameProfileID string value 9268831248 name save game user id uint32 value 1 save name difficulty uint32 value 0 name assist p2 braking uint32 value 0 name assist p2 ABS uint32 value 0 name assist p2 traction control uint32 value 0 name p2 transmission type uint32 value 0 name assist p2 dynamic racing line uint32 value 0 name assist p2 pit limiter uint32 value 0 name assist p2 pit box control uint32 value 0 name assist race braking uint32 value 0 name assist race ABS uint32 value 0 name assist race traction control</td>
</tr>
</tbody>
</table>
Xbox usage data

- Youtube app
- Netflix app
- Xbox Live search app
- Accessed email
- Purchased and downloaded games
Emails on the Xbox
To protect yourself

- Patch your devices
- Don’t click on links in emails or documents
- Avoid using services you could use on traditional computers on non-traditional ones
- Use multi-factor authentication
- Avoid public wifi
- Keep personal information personal
- Educate each other
- Report problems when they occur
If you are a victim of cyber crime

- Notify local authorities immediately
- File a complaint with the Internet Crime Complaint Center [www.ic3.gov](http://www.ic3.gov)
We will never eliminate attacks, but we can take steps to limit their frequency and impact..
Thank you!