Hacked…
Surviving a WEB Attack

Karl Voss
KAET / Eight
karl.voss@asu.edu

What I WILL cover *Hacked…*

- Overview of WEB site vulnerabilities
  - Poor programming practices
  - Improper placement of data
- What happened to KAET?
- KAET's response to the event
- What went right
- What went wrong
- Lessons Learned

What I WON'T cover *Hacked…*

- Web site vulnerabilities
  - SQL Injections
  - Unfiltered user input
  - Remote Code execution
  - Cross Site Scripting
- Forensic examination
  - Servers
  - Logs

What is “PCI”?

Hacked…

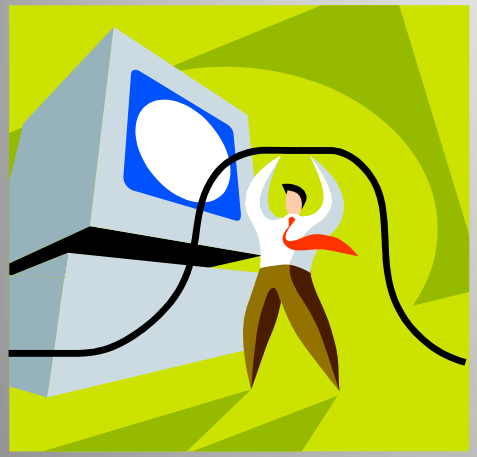
- PCI = “Payment Card Industry”
- PII = “Personally Identifiable Info”
- Good practices even if your servers do NOT contain PII
- Different levels of compliance: If no PII, you don’t have to “do everything”

What is “PII”?

Hacked…

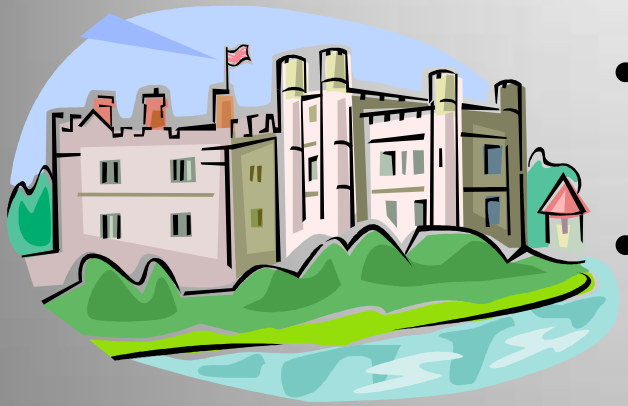
- **Data that should NEVER be on a publicly available server.**
- Personally Identifiable Information. Includes:
  - ✓ Names
  - ✓ Addresses
  - ✓ E-mail addresses
  - ✓ SSN, Driver’s License /Passport info, etc.
  - ✓ Bank info; routing, credit/debit card numbers, CVV numbers

Background *Hacked…*



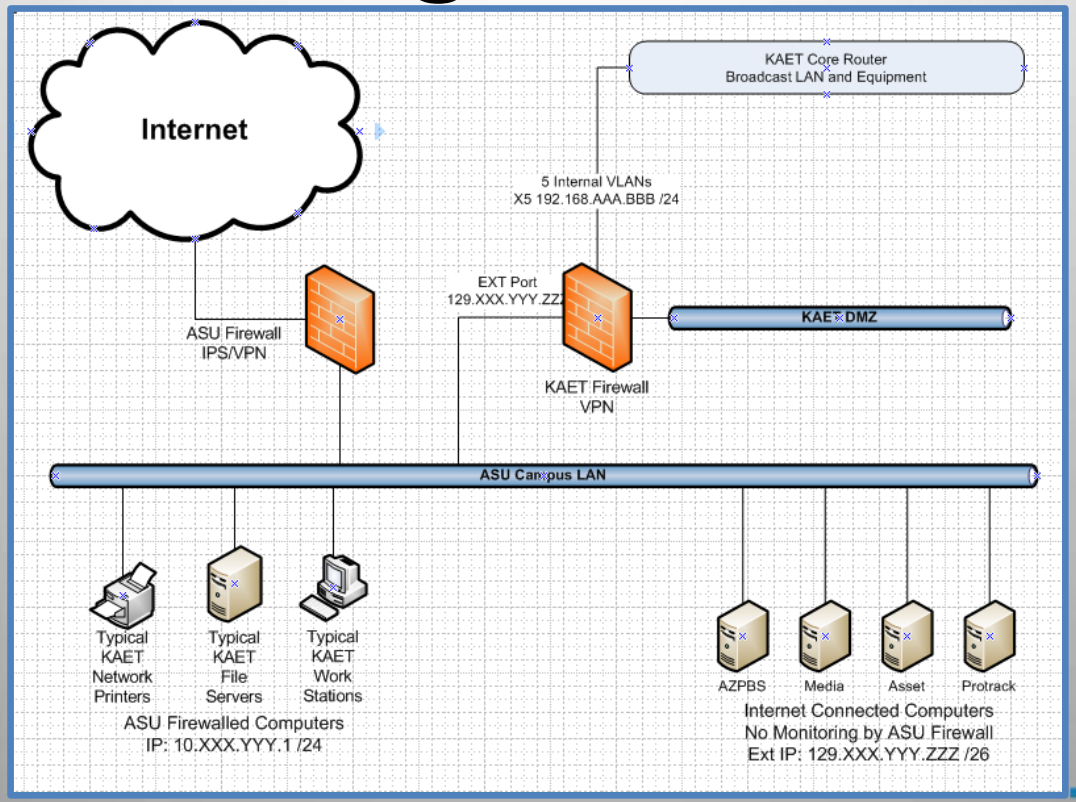
- KAET is generally PCI compliant
- Servers backed up regularly
- Follow “IT Best Practices”
- Apply multiple layers of defenses.

Defense in Depth *Hacked…*



- Physically secured servers
- No users login in with Administrative permissions
- All applications run under restrictive permissions
- Administrative logins are restricted to our IP segment
- Multiple Firewalls – ASU and KAET

Old LAN Configuration *Hacked…*



Programmers *Hacked…*

Table = “members”
“email”,”varchar(100)”
“phone”,”varchar(13)”
“state”,”varchar(2)”
“city”,”varchar(50)”
“address”,”varchar(255)”
“mailingName”,”varchar(255)”
“lastName”,”varchar(50)”
“firstName”,”varchar(50)”
“src”,”int(11)”
“status”,”varchar(1)”
“nameNum”,”int(11)”
“memberNum”,”int(11)”
“id”,”int(10) unsigned”

- Student WEB programmers
- Not aware of input sanitization
- No PII information was *supposed to be* stored on publically accessible computers!

Event Timetable *Hacked…*

- Frontline does story on Wiki Leaks
- PBS.ORG is initially hacked and

Hackers taunt PBS and affiliate web security

- Warning from PBS to affiliates:

6/25/11 3:37p: ”2 affiliate sites hacked”

Event Timetable *Hacked…*

- KAET IT finds Hacker's Twitter feeds

The latest is against http://www.azpbs.org/ with supposedly ~~30K~~ 300K records, which are currently being dumped. The following comes from the PasteBin posting

@Abhaxas
This one will take a while to dump guys..

- Hackers announce "AZPBS is next" after finding an SQL injection bug
- and the "FUN" begins at 6:38p on 6/25/11

KAET's Response *Hacked…*

- ALL servers on Internet were immediately shut off, taken off line & ethernet disconnected –
  - What data did they get?
  - What did they do?
- Expire and change ALL passwords
- Add ACCESS CONTROL LIST to router to restrict future access of ALL servers on the internet to our subnet only – for testing purposes.
- Notify ASU & asked them to maintain ALL log files to preserve evidence

KAET – continued *Hacked…*

- Did a forensic disk image of hacked server before doing ANYTHING else on the server – including powering it up
- Examine the compromised WEB server:
  - What other data was on the server?
  - Why was this data on the server?
  - Was any malware introduced into the server?
- After verifying integrity, put servers back on restricted in-house network – NO PUBLIC ACCESS

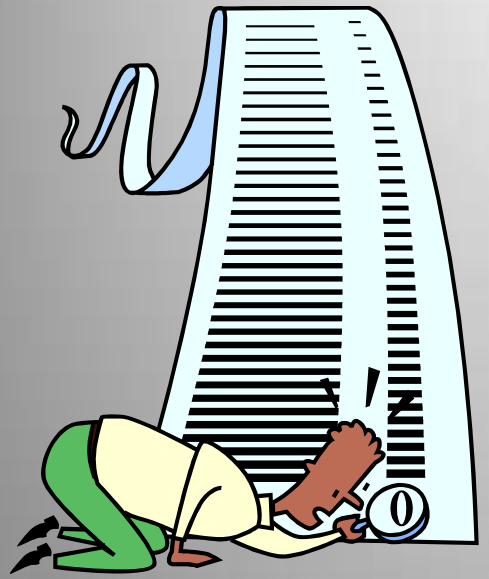
KAET – continued *Hacked…*

- Find and run hacker tools against quarantined computers.
  - 1st run resulted in a 85 page report!
  - Many errors cause multiple “hits” and it didn’t take long to correct the WEB server
- After fixing or disabling all problems identified by hacker tools, put the servers back on line for public access

ASU's Response *Hacked…*

- ASU Help Desk Challenges!
  - Help Desk could NOT expire passwords!
- Took 3 days to "wake the sleeping dog"
- Formed a committee to bring the right people together
- Got legal involved
- Helped draft press responses and letters to all people that had data compromised

Logfile Forensics *Hacked…*



- Examined the log files from our servers
  - Only took 21 seconds to successfully attack the media player!
  - 4 Failed attempts to upload malware
  - 913 records (697 unique households) were downloaded in 3 hours before the WEB server was shutdown
  - Attacker made between 10-30 SQL Injection requests/minute
  - Requested 1 row from the members table at a time – starting from the end of the table and working backwards toward the beginning

SQL Injection *Hacked…*

- Sample normal WEB Input
  `/asuspotlight/player169.php?id=22&episode=105`

- Hacker injected "Bad Input"!

```
/asuspotlight/player169.php?id=22%20AND%20%28SELECT%205045%20FROM%28SELECT%20COUNT%28%2A%29%2CCONCAT%28CHAR%2858%2C118%2C118%2C105%2C58%29%2C%28SELECT%20%28CASE%20WHEN%20%285045%3D5045%29%20THEN%201%20ELSE%200%20END%29%29%2CCHAR%2858%2C110%2C105%2C118%2C58%29%2CFLOOR%28RAND%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.CHARACTER_SETS%20GROUP%20BY%20x%29a%29%20&episode=105
```

- "Bad Input" made human readable

```
/asuspotlight/player169.php?id=22 AND (SELECT 5045 FROM(SELECT COUNT(*),CONCAT(CHAR(58,118,118,105,58),(SELECT (CASE WHEN (5045=5045) THEN 1 ELSE 0 END)),CHAR(58,110,105,118,58),FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) &episode=105
```

KAET – Remediation *Hacked…*

- Identify what info was taken
- Letters to affected members
- Phone Calls to Major Donors
- Issue new member numbers & member cards to affected members
- Remove ALL sensitive information from WEB server

What went right *Hacked…*

- Warning from PBS (June 25, 3:52p)
- IT person was home, available & interested
- Lucky: The Hacker published his “exploits” in real time!
- “defense in depth” kept Hacker from loading evil software on server

What went wrong *Hacked…*

- Database was NOT supposed to be on this server
- Couldn’t expire passwords
- Couldn’t get past ASU’s 1st level support on weekend
- Inactive Intrusion Prevention System (IPS)
- IPS probably wouldn’t find the attack anyway!

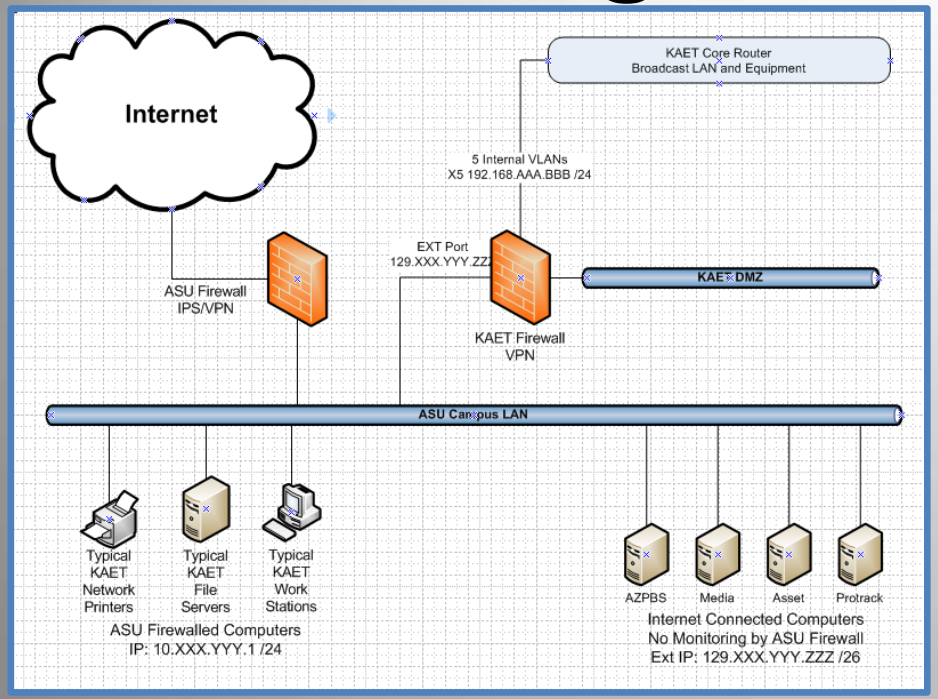
Lessons Learned *Hacked…*

- Take security of your WEB server in house!
- Don’t rely on the “cloud” to protect your assets!
- Don’t rely on your programmers to “be secure” – especially if using students!
- Conduct your own security audits
- Put servers behind your OWN firewall and Intrusion Protection System

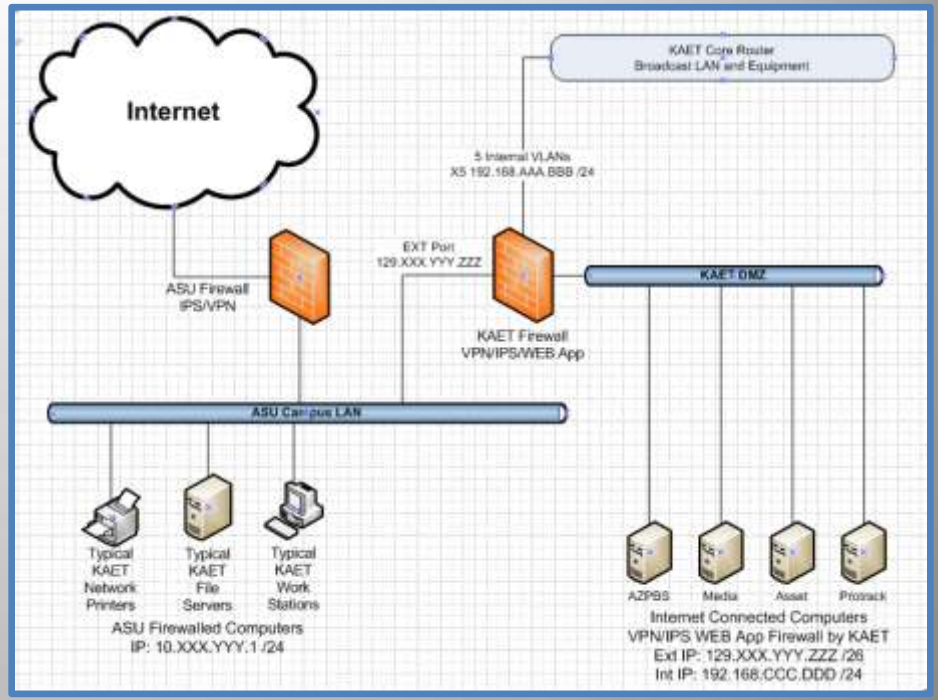
Lessons Learned *Hacked…*

- Eliminate or Encrypt sensitive information on servers
- Keep your staff informed about what happened & what you are doing about it
- Send a letter and setup a “hotline” phone for viewers to contact. Have viewers call the MAIN station number and be sent to the hotline or station management.
- More rules apply if PII is involved!

LAN Changes *Hacked…*



LAN Configuration Before Hack



LAN Configuration After Hack

Policies

Hacked…

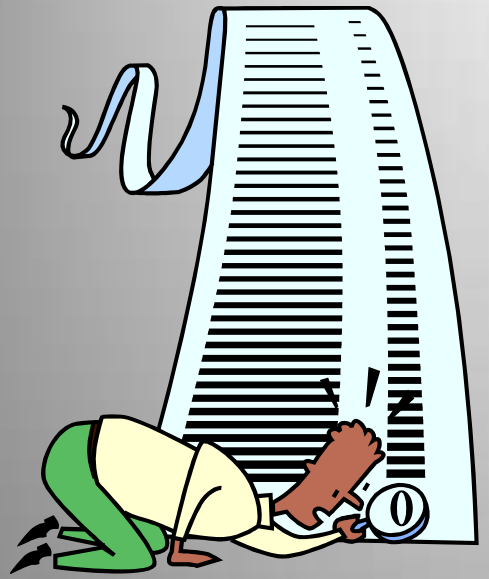
- Put policies in place BEFORE you need them!
- How do you get past the front line “help” desk
- Identify locations of PII
- How do you force password changes?

Passwords *Hacked…*

- how often are they changed
- how secure are they?
- Complex passwords do NOT need to be difficult to remember
  - ⛔ “X7gR4$kK02bQ"
  - ✅ “MAPLE!=banana”

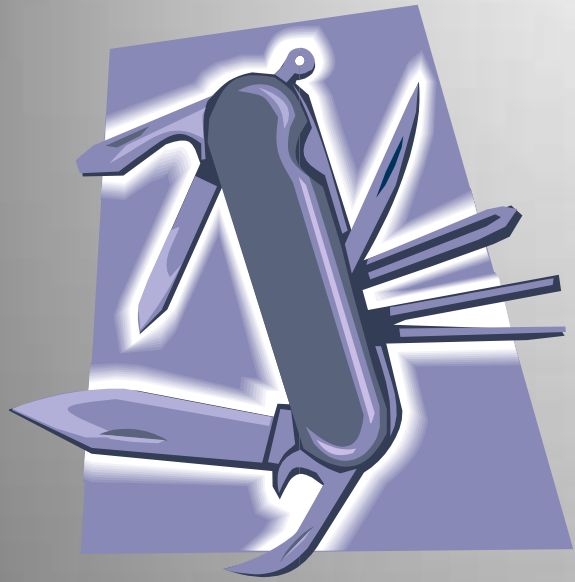
Log files

Hacked…



- Are they turned on?
- Are they looked at on a regular basis?
- Are they stored elsewhere - for how long?

“Hacker” Tools *Hacked…*



- BACKUP your systems BEFORE running the tools
- Make SURE your administrators are aware *BEFORE running them!*
- Run several different tools
- Find and fix the problems that are found

Traps To Avoid! *Hacked…*

- Don’t minimize the implications of the hack to your staff or viewers!
- Especially if no PII, by legal standards, was released!

Does “PCI/PII” Apply? *Hacked…*

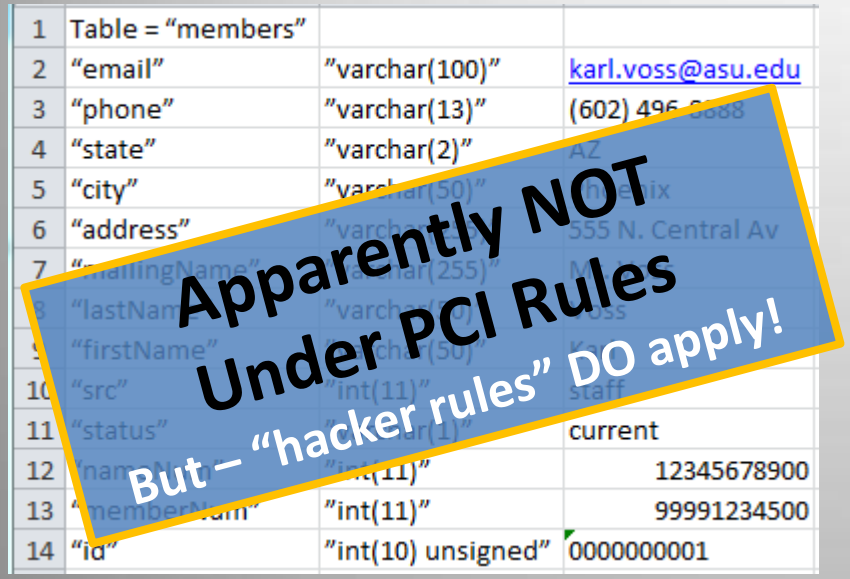
1	Table = “members”		
2	“email”	”varchar(100)”	karl.voss@asu.edu
3	“phone”	”varchar(13)”	(602) 496-8888
4	“state”	”varchar(2)”	AZ
5	“city”	”varchar(50)”	Phoenix
6	“address”	”varchar(255)”	555 N. Central Av
7	“mailingName”	”varchar(255)”	Mr. Voss
8	“lastName”	”varchar(50)”	Voss
9	“firstName”	”varchar(50)”	Karl
10	“src”	”int(11)”	staff
11	“status”	”varchar(1)”	current
12	“nameNum”	”int(11)”	12345678900
13	“memberNum”	”int(11)”	99991234500
14	“id”	”int(10) unsigned”	0000000001

- Personally Identifiable Information. Includes:
  - ✓ Names
  - ✓ Addresses
  - ✓ E-mail addresses

  SSN, Driver’s License /Passport info, etc.

  Bank info; routing, credit/debit card numbers, CVV numbers

Does “PCI/PII” Apply? *Hacked…*



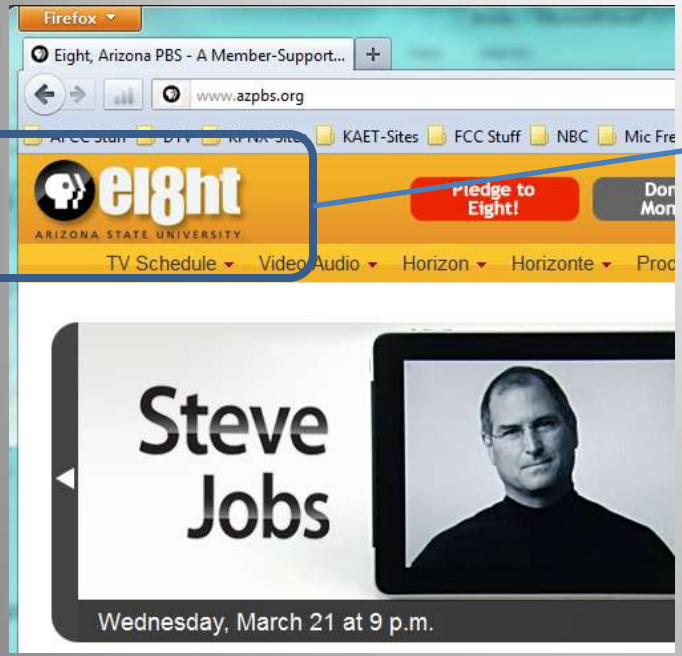
1	Table = “members”		
2	“email”	”varchar(100)”	karl.voss@asu.edu
3	“phone”	”varchar(13)”	(602) 496-[illegible]
4	“state”	”varchar(2)”	AZ
5	“city”	”varchar(50)”	Phoenix
6	“address”	”varchar(255)”	555 N. Central Av
7	“mailingName”	”varchar(255)”	Mr. Voss
8	“lastName”	”varchar(50)”	Voss
9	“firstName”	”varchar(50)”	Karl
10	“src”	”int(11)”	staff
11	“status”	”varchar(1)”	current
12	“[illegible]”	”int(11)”	12345678900
13	“memberNum”	”int(11)”	99991234500
14	“id”	”int(10) unsigned”	0000000001

- Personally Identifiable Information. Includes:
  - ✓ Names
  - ✓ Addresses
  - ✓ E-mail addresses

  SSN, Driver’s License /Passport info, etc.

  Bank info; routing, credit/debit card numbers, CVV numbers

Phishing!

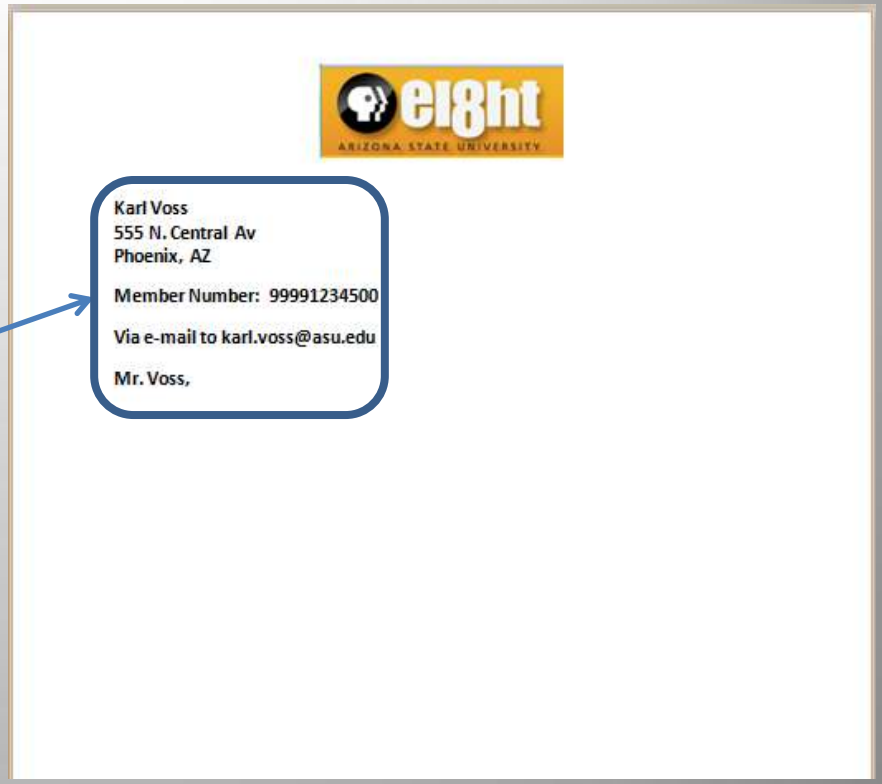


Hacked…

Phishing!

Hacked…

1	Table = “members”		
2	“email”	”varchar(100)”	karl.voss@asu.edu
3	“phone”	”varchar(13)”	(602) 496-8888
4	“state”	”varchar(2)”	AZ
5	“city”	”varchar(50)”	Phoenix
6	“address”	”varchar(255)”	555 N. Central Av
7	“mailingName”	”varchar(255)”	Mr. Voss
8	“lastName”	”varchar(50)”	Voss
9	“firstName”	”varchar(50)”	Karl
10	“src”	”int(11)”	staff
11	“status”	”varchar(1)”	current
12	“nameNum”	”int(11)”	12345678900
13	“memberNum”	”int(11)”	99991234500
14	“id”	”int(10) unsigned”	0000000001



Phishing!

This is a hacker created "phishing message" from YOUR data and YOUR WEB site that would pass the "Karl's Mom Test". In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack – from a legal point of view!

Hacked…

el8ht
ARIZONA STATE UNIVERSITY

Karl Voss
555 N. Central Av
Phoenix, AZ

Member Number: 99991234500

Via e-mail to karl.voss@asu.edu

Mr. Voss,

This is a hacker created "phishing message" from YOUR data and YOUR WEB site that would pass the "Karl's Mom Test". In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack – from a legal point of view!

Phishing!

Hacked…

Karl Voss
555 N. Central Av
Phoenix, AZ

Member Number: 99991234500

Via e-mail to karl.voss@asu.edu

Mr. Voss,

This is a hacker created "phishing message" from YOUR data and YOUR WEB site that would pass the "Karl's Mom Test". In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack – from a legal point of view!

Phishing!

Hacked…

PASSES
the "Karl's Mom Test"
So it MUST be from KAET!

el8ht
ARIZONA STATE UNIVERSITY

Karl Voss
555 N. Central Av
Phoenix, AZ

Member Number: 99991234500

Via e-mail to karl.voss@asu.edu

Mr. Voss,

This is a hacker created "phishing message" from YOUR data and YOUR WEB site that would pass the "Karl's Mom Test". In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack from a legal point of view!

Phishing!

Hacked…

1	Table = “members”		
2	“email”	”varchar(100)”	karl.voss@asu.edu
3	“phone”	”varchar(13)”	(602) 496-8888
4	“state”	”varchar(2)”	AZ
5	“city”	”varchar(50)”	Phoenix
6	“ad	55)”	555 N. Central Av
7	“m	55)”	Mr. Voss
8	“la	)”	Voss
9	“fi	)”	Karl
10	“sr		staff
11	“status	varchar(1)”	current
12	“nameNum”	”int(11)”	12345678900
13	“memberNum”	”int(11)”	99991234500
14	“id”	”int(10) unsigned”	0000000001

el8ht
ARIZONA STATE UNIVERSITY

Karl Voss
555 N. Central Av
Phoenix, AZ

Member Number: 99991234500

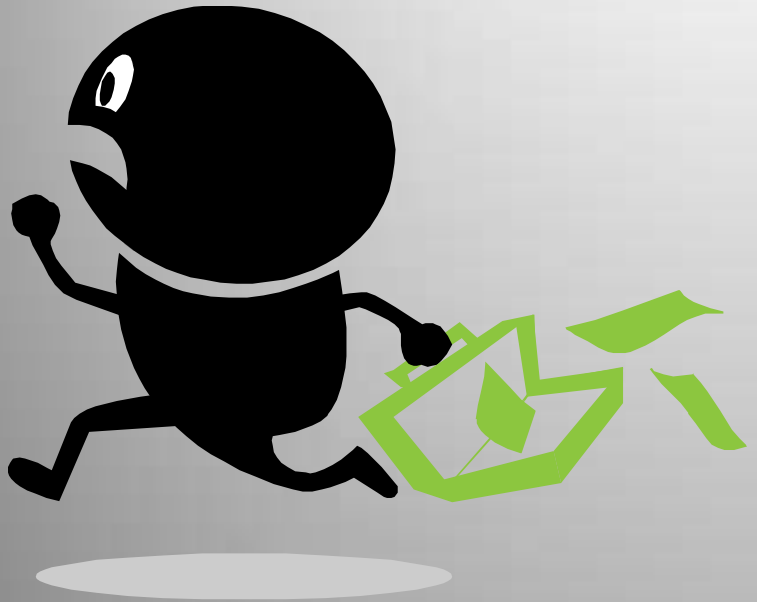
Via e-mail to karl.voss@asu.edu

Mr. Voss,

This is a hacker created “phishing message” from YOUR data and YOUR WEB site that would pass the “Karl’s Mom Test”. In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack – from a legal point of view!

Phishing!



Hacked…

el8ht
ARIZONA STATE UNIVERSITY

Karl Voss
555 N. Central Av
Phoenix, AZ

Member Number: 99991234500

Via e-mail to karl.voss@asu.edu

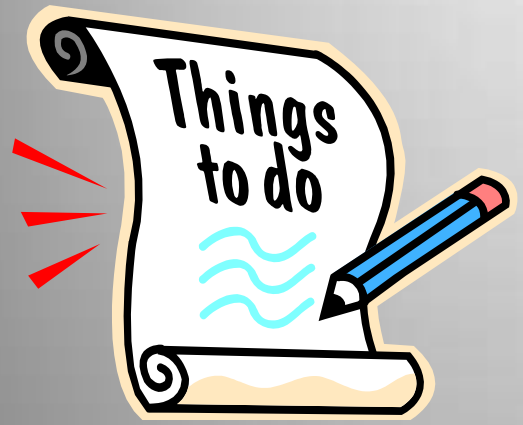
Mr. Voss,

This is a hacker created "phishing message" from YOUR data and YOUR WEB site that would pass the "Karl's Mom Test". In this area, we could come up with a plausible reason to ask the Member to send the hacker their credit card info….

See how easy it would be to mail-merge this message to your membership database if you were hacked and decided NOT to do anything about it! All because there was no Personally Identifiable Information obtained from the hack – from a legal point of view!

Summary

Hacked…



- Inventory your systems on the internet
  - System Configurations
  - What data is on the computers?
  - Anything that should NOT be there?
- Follow General IT recommendations
- Backup your computers
- Keep your computers patched and up to date software wise
- Be prepared for the worst!

Thanks

Hacked…

Questions?

Karl Voss

KAET/Eight

Phoenix, AZ

karl.voss@asu.edu