Overview

- How Information Technology handles E-mail and Spam
- What you can do about E-mail and Spam
- Cloud-based E-mail
What exactly is spam?

- Unsolicited bulk E-mail sent indiscriminately
- Different forms: Unwanted mailing lists, phishing attacks to gain information, form E-mails searching for business
- The name ‘spam’ is derived from the 1970 Monty Python ‘spam’ sketch!
How IT handles E-mail

- Mail Routing - i.e. How does E-mail get into SRJC?
- Server-level Spam detection and blocking
- Maintenance, backups, virus protection, and monitoring
Mail Routing

1. Internet
2. Firewall
3. IronPort
4. SpamAssassin & Virus checking
5. Exchange
6. Client
Mail Routing

- Firewall - Blocks gross spam offenders
- IronPort - Blocks spam offenders based on rules, whitelists, blacklists, with a constantly updated database of known offenders
- SpamAssassin - Filters and blocks spam based on content with additional control based on user preferences
- Virus check - Detects and removes viruses in attachments and bad code in E-mail
Spam Statistics

How much are we talking about?

- Spam prevented at the server
- Potentially good E-mail allowed through

1. Server antivirus scan - strips out bad attachments and bad code

2. Delivered to user for more granular control
Spam Statistics

- Spam prevented at the server
- Potentially good E-mail allowed through

60,000 messages!

This chart just shows one server. It has a twin that is doing the same amount of work. If we only used one, and it stopped working, imagine the number of messages everyone would be bombarded with!
Spam Statistics

- IT dynamically preprocesses roughly 120,000 ~ 150,000 messages each day!
- This yields about 10,000 to 12,000 possibly good E-mails delivered to our mailboxes
E-mail Storage and Backup

- IT backs up E-mail every night
- Retention policies in place
- Rough cost per terabyte (TB) ~ $14,000
- Enterprise grade hardware
- Redundancy
Questions?

Coming up: what you can do about spam
What You Can Do About Spam

1. Set SpamAssassin Preferences
2. Client Filters or Rules
3. Identifying E-mails
4. E-mail in Context
1. SpamAssassin
SpamAssassin

Scans and marks E-mail based on content at the server level

- **E-mail Score** - Each E-mail is scored based on the content of the message
- **Whitelist / Blacklist** - Users can specify who can send them E-mail and who cannot
Weird repeated double-quotations marks

Attempts to disguise the word 'viagra'

Subject is all capitals

Message body has 80-90% blank lines

Subject contains "Your Bills" or similar

Subject contains a gappy version of 'xanax'

Talks about price per dose

Attempts to obfuscate words in spam

Over 700 of these E-mail body and header tests are run per message!

Join Millions of Americans

Subject line starts with Buy or Buying

SpamAssassin Scores Based on Content

Sender is confirmed spam source

Talks about lots of money

Talks about Oprah with an exclamation!

Subject contains "Your Family"

Information on getting larger body parts
SpamAssassin Scores

- Any time content matches a test, SpamAssassin adds a number to the score.
- The higher the score an E-mail receives, the more “spammy” a message seems.
- Note: SpamAssassin ignores E-mail’s that are sent to multiple recipients.
Setting SpamAssassin Scores

- On your personal SpamAssassin preferences, you can set the score a message must receive before being tagged as spam
  - A larger score means more “spammy” content gets through - less E-mails are marked as spam
  - A smaller score means less “spammy” content gets through - more E-mails are marked as spam
SpamAssassin Example E-mail

SpamAssassin identified this as spam by using asterisks and the word SPAM in the title.

Notice the scores on the left side.
Whitelist / Blacklist

- **Whitelist** - Always allows E-mail from someone you have approved, despite a high SpamAssassin score

- **Blacklist** - Never allows E-mail from someone you have denied
## SpamAssassin Preferences

Logged in as: mberger (log out)

### Allow / Deny Addresses List

Below is your list of sender addresses that are either **Allowed** or **Denied** passage regardless of the Spam score.

<table>
<thead>
<tr>
<th>Address</th>
<th>Type</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Allow</td>
<td>Delete</td>
</tr>
<tr>
<td></td>
<td>Allow</td>
<td>Delete</td>
</tr>
</tbody>
</table>

#### Add New Address

Address: 
Type:  
- Allow
- Deny

#### General Settings

Once all SpamAssassin tests have been run, the resulting score is matched against this value, and if greater than this value, the email message is marked as spam.

**Required Hits**

The default value for Required Hits is 5, which is quite aggressive. A value of 10 will produce less false positives. The average SPAM score is around 15 to 16.
SpamAssassin Preferences Demo!
2. Client Filtering
“Good rule of thumb: When you check your email and find yourself groaning "Ugh, this again?" consider creating a filter. A filter is ultimately best at shunting away the really unimportant stuff -- you are the only one who's got the qualifications and wetware to decide what happens to important items. That's why you get the big bucks.”

-Merlin Mann, 43 Folders
Client Filtering

- Not all of us can achieve Inbox Zero, but we can strive to get close
- Filters or rules allow us to tailor what we see and when
- Filter based on subject, sender, message content, and much more
How to set up Client Filters or Rules

santarosa.edu/email/rules
Rule Examples

- Tell your students to always place your class section number in the subject line and then filter them into a folder
- Filter specific people or groups of people into folders to help keep track of different departments or projects
- Filter mailing lists and newsletters
Rules Demo!
3. Identifying E-mail

- E-Mail Spoofing
- Phishing Attacks
  - Domain Name Grammar
- E-mail Lists
- Canned (Form) E-mail
E-mail Spoofing

- Sender address and other parts of the E-mail are altered to appear as though the E-mail originated from a different source
- The E-mail protocol SMTP doesn't provide any authentication - it’s easy to impersonate and forge E-mails
- SMTP - Simple Mail Transport Protocol (key word here is ‘Simple’)
- Can originate from spammers directly or malware/spyware infested ‘Zombie computers’
E-mail Spoofing

- **Zombie computer** - a compromised computer under the control of a computer program to gather data

- For example, this can cause a local computer address book to become compromised, allowing spammers to send E-mails to people in the address book

- Receivers think it is someone they know sending them an E-mail, but it really is a malicious program

- **Joe Job** - Flood of a huge number of E-mails from a spoofed address, i.e. - denial of service attack
How to Stop E-Mail Spoofing

- You can’t
- It is, unfortunately, one of the main issues in E-mail
- If you know the person (friend, student, etc) contact the “sender” via another method (phone, etc.) to let them know their computer may be compromised

- DO: Use rules and SpamAssassin
Phishing Attacks

- E-mails specifically targeted to fool you into giving up information
- They ask for usernames, passwords, login information, credit card numbers, and more
- Examples: Banking sites, mortgage offers, ‘Help Desk’ account has expired, credit report information
- Never respond to a phishing attack
- Spear Phishing - Directed ‘attack’ with personal information included, harder to detect!
So, how can we tell if it is a phishing attack?
-----Original Message-----
From: Rita [mailto:mesacc.edu]
Sent: Tuesday, July 26, 2011 11:21 AM
Subject: Mailbox Upgrade

Attn: Faculty/Staff/Students,

This message is from our Helpdesk Team to all webmail account owners.

We noticed that your webmail account has been compromised by spammers. It seems they have gained access into our database and have been using it for illegal internet activities.

The center is currently performing maintenance and upgrading its database. We intend upgrading our Email Security Server for better online services.

To re-validate your mailbox and upgrade your account, please click below

http://www.my3q.com/go.php?url=upgrad7543/9400

In order to ensure you do not experience service interruptions, please upgrade your account to prevent it from being deactivated from our database.

Thank you for using our online services.
Rita
For Helpdesk Team
-----Original Message-----
From: Rita [mailto:s@mesacc.edu]
Sent: Tuesday, July 26, 2011 11:21 AM
Subject: Mailbox Upgrade

Attn: Faculty/Staff/Students,

This message is from our Helpdesk Team to all webmail account owners.

We noticed that your webmail account has been compromised by spammers. It seems they have gained access into our database and have been using it for illegal internet activities.

The center is currently performing maintenance and upgrading its database. We intend upgrading our Email Security Server for better online services.

To re-validate your mailbox and upgrade your account, please click below

http://www.my3g.com/go.php?url=upgrad7543/9400

In order to ensure you do not experience service interruptions, please upgrade your account to prevent it from being deactivated from our database.

Thank you for using our online services.
Rita
For Helpdesk Team
Phishing Attack Example 2

---

From: Mary [mailto:...@cornell.edu]
Sent: Wednesday, April 27, 2011 6:15 PM
To: li@s.com
Subject: Mailbox Alert

This is to notify you that you are over your mailbox limit which is 250MB as set by your mailbox manager, you are currently at 257MB, you will not be able to create new e-mail to send or receive messages until you validate your mailbox. To re-validate your account, click here:

Thank You.
IT Help Desk.

---

From: Mary [mailto:...@cornell.edu]
Sent: Wednesday, April 27, 2011 6:15 PM
To: li@s.com
Subject: Mailbox Alert

This is to notify you that you are over your mailbox limit which is 250MB as set by your mailbox manager, you are currently at 257MB, you will not be able to create new e-mail to send or receive messages until you validate your mailbox. To re-validate your account, click here:

Thank You.
IT Help Desk.
Phishing Attacks - Hidden Links

1. DO NOT click the link

2. Hover your mouse cursor over the link

3. In this example, that “click here” link would have taken you to http://azxdjuv.tk

4. This is obviously NOT www.santarosa.edu and NOT cornell.edu either!
Compare these to a real example:
Your SRJC domain password expires in one month, on Mon Aug 1.

noreply@busadmin.santarosa.edu
Sent: Sunday, July 3, 2011 12:08 AM
To: [redacted]

Your SRJC domain password expires in one month, on Mon Aug 1.

This expiration notice is for the account named: [redacted]

When changing your password, the new password must meet these criteria:
1. At least one UPPERCASE letter, one lowercase letter, and one number/symbol.
2. The password must consist of at least six characters.
3. The password cannot be the same as any password previously used at SRJC.
4. The password cannot contain parts of your first name, last name, or your username.
5. Only ONE successful password change is allowed in a TWENTY-FOUR HOUR period.

PASSWORD CHANGE INSTRUCTIONS

PLEASE NOTE: If you use a Mac on Campus, you MUST change your password ON CAMPUS to avoid "keychain" problems.

PC (On Campus ONLY)
1. Login to your computer through the normal process (Ctrl + Alt + Del).
2. Once you are logged in, push Ctrl + Alt + Del again, and you will get a window with several choices.
3. Click on Change Password. Enter your Old Password, New Password, and verify the New Password. Click OK.

Mac (On Campus ONLY)
1. Login to your computer through the normal process.
2. Click on the Apple Menu in the upper left corner, select System Preferences. Double click on the Accounts icon.
3. Click on the Change Password Button. Enter your Old Password, New Password, and verify the New Password.
4. Click OK if you get a dialog about your "Keychain Password" being updated.

PC or Mac (Off Campus)
1. Open a web browser and enter the URL: http://www.santarosa.edu/outlook.
2. Click on Outlook Web Access. Login per normal procedure. Click on Options in the upper right of the screen.
3. In the menu on the far left, scroll down to, and click on Change Password.
4. Enter your Old Password, New Password, and verify the New Password. Click on "Save" ABOVE the form.

If you are unable to change your password:
Contact the help desk during normal working hours via telephone - (707)524-1765.
At that time you will be re-verified as an active employee and your password will be changed.

Remember that we will never ask you for your password via email or over the telephone. Any email correspondence from our department will only use a "santarosa.edu" address.
For your protection against identity theft, never give out your password. Beware of any telephone or email attempts to gather information about you or your account.

The IT personnel cannot see or tell you what your password is, we can only reset the password.

Thank you,
SRJC Information Technology
Your SRJC domain password expires in one month, on Mon Aug 1.

noreply@busadmin.santarosa.edu

Sent: Sunday, July 3, 2011 12:06 AM

To: user@example.com

Your SRJC domain password expires in one month, on Mon Aug 1.

This expiration notice is for the account named: username

When changing your password, the new password must meet these criteria:
1. At least one UPPERCASE letter, one lowercase letter, and one number/symbol.
2. The password must consist of at least six characters.
3. The password cannot be the same as any password previously used at SRJC.
4. The password cannot contain parts of your first name, last name, or your username.
5. Only ONE successful password change is allowed in a TWENTY-FOUR HOUR period.

PASSWORD CHANGE INSTRUCTIONS

PLEASE NOTE: If you use a Mac on Campus, you MUST change your password ON CAMPUS to avoid "keychain" problems.

PC (On Campus ONLY)
1. Login to your computer through the normal process (Ctrl + Alt + Del).
2. Once you are logged in, push Ctrl + Alt + Del again, and you will get a window with several choices.
3. Click on Change Password. Enter your Old Password, New Password, and verify the New Password. Click OK.

Mac (On Campus ONLY)
1. Login to your computer through the normal process.
2. Click on the Apple Menu in the upper left corner, select System Preferences. Double click on the Accounts icon.
3. Click on the Change Password Button. Enter your Old Password, New Password, and verify the New Password. Click OK if you get a dialog about your "Keychain Password" being updated.

PC or Mac (Off Campus)
1. Open a web browser and enter the URL: http://www.santarosa.edu/outlook.
2. Click on Outlook Web Access. Login per normal procedure. Click on Options in the upper right of the screen. http://www.santarosa.edu/outlook
3. In the menu on the far left, scroll down to, and click on Change Password.
4. Enter your Old Password, New Password, and verify the New Password. Click on "Save" ABOVE the form.

If you are unable to change your password:
Contact the help desk during normal working hours via telephone - (707)524-1765.
At that time you will be re-verified as an active employee and your password will be changed.

Remember that we will never ask you for your password via email or over the telephone. Any email correspondence from our department will only use a "santarosa.edu" address.
For your protection against identity theft, never give out your password. Beware of any telephone or email attempts to gather information about you or your account.

The IT personnel cannot see or tell you what your password is, we can only reset the password.

Thank you,

SRJC Information Technology
Dealing with Phishing Attacks

1. Learn how to detect a phishing attack
   A. Information from IT has links and E-mail addresses that reference santarosa.edu
   B. IT will never ask for your password
   C. If it is a bank you are associated with, contact the bank directly, not via any links in the E-mail

2. Communicate with coworkers
   A. Sometimes many people get the same E-mail at the same time

3. NEVER respond to a phishing attack, delete the E-mail

4. Use the SpamAssassin blacklist
## Domain Name Grammar

### www.santarosa.edu /it

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>www</td>
<td>Server</td>
</tr>
<tr>
<td>santarosa</td>
<td>Domain</td>
</tr>
<tr>
<td>edu</td>
<td>Top Level Domain (TLD)</td>
</tr>
<tr>
<td>it</td>
<td>Directory of files to display</td>
</tr>
</tbody>
</table>

Easy trick to figure out where you are: **Ignore everything after a slash, read right to left.**

1. Domain name and Top Level Domain (TLD) are a unique identifier
2. Santa Rosa Junior College TLD is: **.edu**
3. Santa Rosa Junior College full domain name is: **santarosa.edu**
4. Used in URLs for Web sites as well as in E-mail addresses
# Domain Name Grammar

**Examples of safe and spoofed domains**

<table>
<thead>
<tr>
<th>Domain Name</th>
<th>Result</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.santarosa.edu/it">www.santarosa.edu/it</a></td>
<td>✓ OK!</td>
<td>IT Web site</td>
</tr>
<tr>
<td>securemail.santarosa.edu</td>
<td>✓ OK!</td>
<td>E-mail server</td>
</tr>
<tr>
<td>online.santarosa.edu</td>
<td>✓ OK!</td>
<td>Distance Education Web site</td>
</tr>
<tr>
<td>santarosa.edu.ca</td>
<td>✗ NOT OK!</td>
<td>.ca is TLD for Canada</td>
</tr>
<tr>
<td>domain.com/santarosa.edu</td>
<td>✗ NOT OK!</td>
<td>Anything after slash = directory, this is domain.com, not santarosa.edu</td>
</tr>
</tbody>
</table>
E-Mail Lists

- If you are sure you subscribed to a list that you do not want to be a part of any longer, it is most likely okay to unsubscribe using the links in the E-mail

- Never unsubscribe from E-mail lists that you do not recognize - spammers look for legitimate E-mail addresses
Canned or Form E-mail

- Legitimate businesses sending bulk spam E-mails asking for business
- For example, IT receives E-mails all the time from software and hardware vendors, computer training companies, etc.
- Not necessarily spam?
- When in doubt - search online!
4. E-mail in Context

Use your SRJC E-mail address for SRJC business only

Do not use your SRJC E-mail address for social networking sites, shopping sites, and/or personal use

Believe it or not: Legitimate companies DO sell your E-mail address!
Use an Alternate E-mail for Personal Use

- You can always sign up for a free E-mail account for personal use
- Free E-mail sites: Gmail, Yahoo, Windows Live, etc.
- Most likely you have an E-mail address through your ISP - Comcast, AT&T, Sonic.net, etc.
How does my E-mail address get on the spam lists?

- Social Networking sites - Facebook, etc.
  - Social Networking embedded applications - surveys, games, etc.
- Shopping sites
- Published on any search engine friendly Web site (99% of them) - for example, santarosa.edu
- E-mail lists - newsletters for various companies
Cost of Social Networking

For bundles of 1000 accounts:

- Facebook account with 10 friends or less - $25
- Facebook account with 10 or more friends - $45
- How the spammer feels after sending 100,000 E-mails gained from hacked accounts? - Priceless

Source: Verisign iDefence, [http://dealbook.nytimes.com/2010/05/03/stolen-facebook-accounts-for-sale/?src=bulsn](http://dealbook.nytimes.com/2010/05/03/stolen-facebook-accounts-for-sale/?src=bulsn)
Key Things to Remember

That was a lot of information!

Three simple takeaways:

1. Be alert and aware - take a moment to examine the E-mails you receive

2. Use rules to filter messages

3. Set your SpamAssassin preferences
Cloud-based E-mail

- E-mail managed and hosted offsite
- Not going into detail today
- Google Gmail, Microsoft Office 365, etc.
- We are looking into it
# Cloud-based E-mail

**Pros**
- Larger storage
- Ubiquitous access
- Less administration (*)
- Spam prevention
- Cost savings (*)

**Cons**
- Training impact
- Backup and restore ($$)
- Client support
- Network integration
- Legal requirements

* Depending on outcome of our pilot testing
Questions?
# Online Resources

Main IT Web site: [santarosa.edu/it](santarosa.edu/it)

E-mail Web site: [santarosa.edu/email](santarosa.edu/email)

<table>
<thead>
<tr>
<th>Resource</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>SpamAssassin Preferences</td>
<td><a href="santarosa.edu/email/spam/prefs">santarosa.edu/email/spam/prefs</a></td>
</tr>
<tr>
<td>How to create E-mail rules</td>
<td><a href="santarosa.edu/email/rules">santarosa.edu/email/rules</a></td>
</tr>
<tr>
<td>How to archive E-mail</td>
<td><a href="santarosa.edu/email/archive">santarosa.edu/email/archive</a></td>
</tr>
<tr>
<td>Smartphone Information</td>
<td><a href="santarosa.edu/it/support/smartphones">santarosa.edu/it/support/smartphones</a></td>
</tr>
</tbody>
</table>