About Us

- We are a volunteer-based organization that is spreading cyber awareness and creating a cyber first responders unit.
Competing

- We participate in several team-based competitions a year to serve as training and experience to members. (Panoply, CCDC, Mitre)
What we do

- We serve the community as a cyber first responder team.
- Serve as Mentors for Middle Schools/High Schools
- Network with other companies and organizations to create professional relationships
Member Development

- Develop the skills necessary for working in the field of Information Technology.
- Develop good ethics necessary to present themselves as an IT professional.
- Develop cyber security awareness
The Real World
Facebook and Twitter

• Attack occurred in late January.
• None of its users compromised (more than a Billion)
• Caused by a number of its employees visited a compromised website.
• Twitter was also hacked and 250,000 of its users were compromised
• Encrypted e-mails and passwords were stolen
• Caused by the scripting/coding exploit from Java.
Smartphone Attack

• 5 Japanese were arrested for a malicious video app that they released.
• The app was downloaded 270,000 times and stole 10 million pieces of information.
• The malware would transmit phone numbers and e-mails to an external server.
• A similar incident also happened earlier that year in which 6 Japanese funneled $265,000 from smartphone users.
USB attack vector

• USB attacks have been used for infecting an unknowing users with viruses
• Attackers usually drop infected USBs in parking lots
• Malware usually records and installs key loggers in the computer and then sends the info to a external server
E-mail Attacks

• Attackers usually send fake e-mails en-masse to thousands of users with malware.
• E-mails could also be made to “look legit” to fool the users to steal personal information.
• Yahoo Xtra was recently hacked due to e-mail spamming and approximately 450,000 accounts were compromised.
Physical Security

• A clinic customers information was recently stolen due to inadequate physical security
• Papers that were supposed to shredded were stolen by the cleaning service employee that the clinic contracted
• Information that was stolen included name, date of birth, billing info, social security and many more
E-MAIL SECURITY

By: Julian Rios
Companies will never ask you for personal information.

- If personal information is brought up in a non-face-to-face capacity.
- Malicious users impersonate big websites and ask for your information in order to “fix” your account.

![Phishing Scams Example Image]
Email Links

- Links could lead you anywhere.
  - Some links could be safe, others could be swarming with viruses and malware.
  - Always visit websites directly if the email seems trustworthy.
    - E.g. Bank.

- ONLY exception is when you are expecting the e-mail link.
E-mail attachments can be dangerous, no matter who they come from.
Beware of unsolicited attachments.
Keep software and system up to date.
Before opening attachments, save and scan.
Free E-mail Services

- E-mail services like Yahoo, Hotmail, and Gmail.
  - Can be unsafe to use.
  - Enable option for secure browsing, or SSL.
- Messages may be sent in “plain text” and be intercepted by malicious users.
- Avoid sending sensitive information through free e-mail services.

Secure Browsing:

- Keep the connection encrypted while I'm logged in.

Check this box only if you collect sensitive information with your form(s) and intend to browse it on FormAssembly.com.
Avoid sending sensitive information through e-mail.
  - E.g. – Social security, credit card number, etc.
Set up filters for unwanted spam messages.
Don’t access your e-mail from public networks.
  - E.g. – restaurants, cafés, airports, etc.
Spam

- Biggest single threat in e-mail.
  - Millions of e-mail messages are sent out everyday.
  - Spam messages can contain many dangerous attachments.
    - E-mail providers like Hotmail and Gmail have spam filters.
Credits

- http://www.makeuseof.com/tag/7-important-email-security-tips-you-should-know-about *
- www.us-cert.gov/ncas/tips (Computer Emergency Readiness Team)
MALWARE: 
THE HIDDEN PREDATOR

By: Daniel Lopez
What is malware?

- Malware is a generic term to describe any malicious computer code that may perform denial of service, perform spying on a user or cause damage to your system.
Adware

- Delivers advertising content in unexpected manner
- Usually may cause no actual harm to the system
- More nuisance than threat
Spyware

- Used to track user’s viewing history and keystrokes
- Collect personal information about user
- Change computer configurations
- Negative effects of spyware
  - Slow performance
  - New browsers toolbars
  - Hijacked Homepage
  - Increased pop-ups
Keyloggers

- Used to capture exact keystrokes of user
- Method of stealing personal information and user accounts
- May be installed in either a software or hardware method
Trojan Horses

- Technique used to make a program appear legitimate yet may have adverse effects
- Common problems include
  - Open backdoors
  - Transmit data to attack of user
  - Slow system performance
Rootkits

- Set of tools created to hide the presence of other forms of software
- Very hard to find and remove once placed in a system
- Ability to change the entire function of operating system to hide itself
Spam

- Popular method of spreading malware into other systems
- Reduces work productivity
- Nuisance
Social Engineering

- Phishing - attacker impersonating a legitimate business to steal information about user
- Vishing – Similar method but instead though a telephone call
- Impersonation – Impersonate fictitious character. Relies on attackers manipulation of human nature
Any questions?
FIREWALLS

Ashton-Drake Giddings

HTTP://WWW.CYBERTIGERS.ORG
WHAT IS A FIREWALL?

• “A firewall can either be software-based or hardware-based and is used to help keep a network secure. Its primary objective is to control the incoming and outgoing network traffic by analyzing the data packets and determining whether it should be allowed through or not, based on a predetermined rule set.” -Wikipedia
SOFTWARE FIREWALLS

- Microsoft Built-in Firewall
- Linux Built-in IPTables
- ZoneAlarm
- Comodo
WHY IS A FIREWALL IMPORTANT?

• You want to make sure your information is private. You want to make sure unauthorized people don’t access your information from the web. This is why you use a firewall. A firewall will block unauthorized connections.
Windows Firewall is helping to protect your PC

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

On (recommended)
This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

Don't allow exceptions
Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

Off (not recommended)
Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

What else should I know about Windows Firewall?
Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

**Domain Profile**
- **Windows Firewall is on.**
- **Inbound connections that do not match a rule are blocked.**
- **Outbound connections that do not match a rule are allowed.**

**Private Profile is Active**
- **Windows Firewall is on.**
- **Inbound connections that do not match a rule are blocked.**
- **Outbound connections that do not match a rule are allowed.**

**Public Profile is Active**
- **Windows Firewall is on.**
- **Inbound connections that do not match a rule are blocked.**
- **Outbound connections that do not match a rule are allowed.**

**Getting Started**

**Authenticate communications between computers**
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPSec).

**Connection Security Rules**

**View and create firewall rules**
Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if the client is authenticated by IPSec.
ZoneAlarm Security Alert

CHANGED PROGRAM

Opera Internet Browser is trying to access the Internet.

Identification: Not available in ZoneAlarm
Application: Opera.exe
Destination IP: 64.233.163.104:DNS

More Information Available:
This program has changed since the last time it ran!

SmartDefense Advisor

Want to have fewer alerts?
Find out how.

- Remember this setting

[Allow] [Deny]
ONE IS ENOUGH

• Just what the title says. You only need one firewall. Multiple firewalls will conflict. This will then either close down your network completely or open it up completely. It is just safer to have one firewall. Just configure the firewall correctly.
SAFE BROWSING

Ashton-Drake Giddings
GET RID OF THOSE BAD BROWSING HABITS

- Do you trust every link?
- Do you believe e-mails?
- Do you click on links without knowing where they really go?
- Do you not pay attention to the URL address bar?
- Have you ever clicked a message that looked like this:

![Image of a system security alert]

If you answered yes to any of these questions then you should reconsider your browsing habits.
BE AWARE

NOTE that the domain is not a VCU domain but a domain outside of the US

From: "Virginia Commonwealth University <peter.Loeffelmeier@t-online.de>
To:
Date: 02/26/2012 05:35 PM
Subject: New Secure Message Regarding Your Virginia Commonwealth University Webmail

Dear valued customer,
You have 1 new Security Message Alert!
Log In into your account to update your profile.
Click here to Log In

Virginia Commonwealth University.
FALSE LINKS

Retrieving pictures was prevented to protect privacy. The email was sent from Twitter to geoff.duke@uvm.edu on Tue 3/22/2011 3:24 AM. The subject is "You have notifications pending".

Hello,

You have notifications pending
http://twitter.com/account/notify/4438E-C2798-936741?emcamp=notify_20110322&userid=577939563

Click to follow link

Thanks for being part of Twitter,
The Twitter Team
MISSPELLING AND GENERALIZATION

Password change required!

Dear sir,

We recently have determined that different computers have logged onto your eBay account, and multiple password failures were present before the logons. We strongly advice CHANGE YOUR PASSWORD.

If this is not completed by September 30, 2006, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. Thank you for your cooperation.

[Click here to Change Your Password]
If you’re using a website that you’re inserting private information (I.E. Facebook, Bank websites, E-Commerce), always use HTTPS. This ensures a more secure connection and encrypts your data (passwords, credit card number).
UPDATE YOUR BROWSER

• Just like any other piece of software, you want to keep up to date. A lot of the updates are made to fix bugs and security flaws.
PUBLIC NETWORKS

• Don’t put your important information on public networks
• Ex: Hotels, McDonald’s, Starbucks