Cybersecurity Information Session

Computer Services

NSCAD University

March 2, 2017

Overview

- Security takes priority
- Higher Education at risk
- Types of attack
- NSCAD protection
- Actions that reduce risk
- Privacy and Security
- Questions?

Ready market for personal information. One figure quoted 50 cents per record, meaning that the theft of 100,000 records yields a $50,000 profit

Board members and executives have been fired and publicly chastised for failing to perform their due diligence (e.g. Target, Sony, Wells Fargo)

As per recent studies, about half of tested subjects click on links from strangers in e-mails and Facebook messages—even though most of them claim to be aware of the risks – illustrating the breadth of vulnerability and the limitations of user education

Privacy breaches are far reaching and can have unexpected outcome

*Security takes priority

*Higher Education at risk

Open scholarly communication - often coupled with decentralized systems, structures and decision-making authority that are seen as supportive of academic freedom - can make universities easier to attack and exploit than other entities. ***(Soft targets)***

Institutions of all sizes retain thousands and sometimes millions of personal records containing personally identifiable information (PII), payment card information (PCI) and protected health information (PHI), all of which have value to hackers. ***(Privacy and liability concerns)***

The University of Calgary ransomware experience is well known within Canadian university circles. The University paid a $20,000 ransom. Other direct and indirect costs were also incurred.

The University of Maryland reported that it lost the records of 300,000 current and former students and spent $2.6M on credit monitoring and estimated its total cost for "reorganization and new security protections" at $20M.

NSCAD's external firewall currently fields about 20,000 hack attempts per week

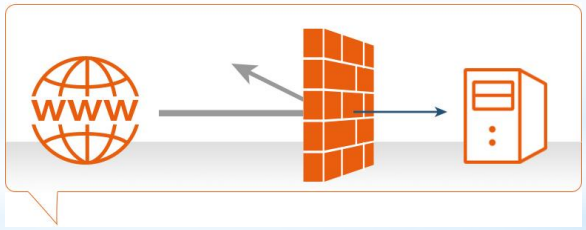
*Higher Education at risk

Types of attack

- **Malware:** software created with malicious intent
- **Phishing:** use of disguise to obtain sensitive information
- **Ransomware:** malware designed to block access to a computer system until a sum of money is paid
- **Trojan:** malware that misleads users as to its true intent
- **Virus:** malware that spreads by attaching itself to an existing program
- **Worm:** standalone malware that replicates itself in order to spread to other computers

NSCAD's external firewall

* NSCAD's external firewall is our main defense for threats coming from the outside in
* It fields about 20,000 hack attempts per week
* It is very lean and allows very little access



* NSCAD protection

Email Filtering

* All email passes through the best spam filters and anti-virus software available (Microsoft Office 365)
* Supported by an army of programmers, these services block over 90% of all email directed at us
* Email is always blocked when the origin of the email is known to be a reported spammer or malware distributer
* Email is often blocked if the origin of the email cannot be verified

NSCAD protection

Internal Firewalls

* All internally-provided NSCAD services run on servers or appliances with individual, sophisticated, up-to-date firewalls
* These firewalls are professionally programmed and frequently tested
* Our servers are monitored for perfomance

NSCAD protection

Individual Equipment Protection

* All NSCAD owned Macs and PCS are now provided with Avast! Anti-virus pre-installed
* All NSCAD Macbooks, Laptops and Notebooks are now provided fully encrypted
* Compliance is monitored

NSCAD protection

Internal network separation

* NSCAD has separate networks for Administration, Security, Academics, Secure Wireless and General Wireless
* NSCAD applies separate, enforceable rules regarding access to each network

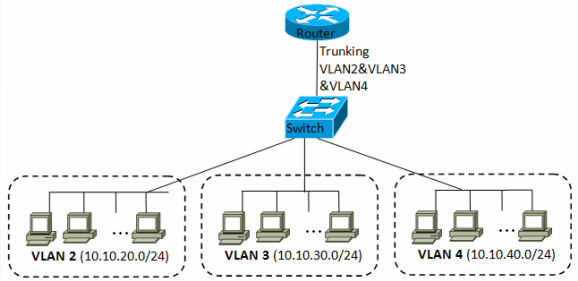
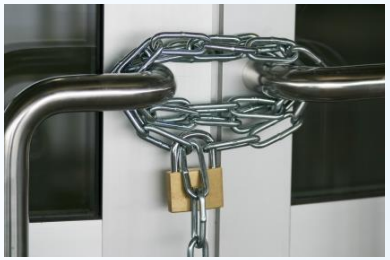


Figure 12.5. 802.1Q trunk between the router and the switch

* NSCAD protection

Physical security is important

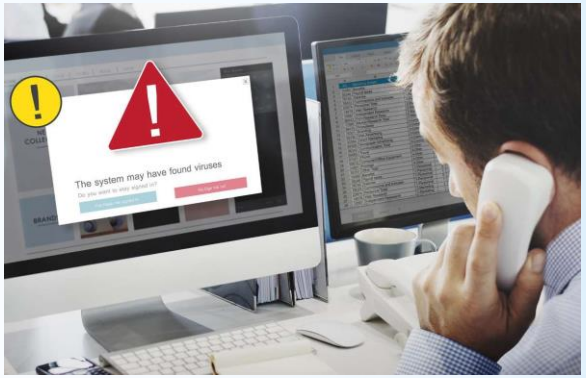
* Make sure the physical location(s) of your computer equipment are secure. Once someone gains physical possession of a computer or device, **nothing** can stop them from using it. The hacks to gain administrative rights are on the internet and easily accessible.



* Actions that reduce risk

What you need to have installed

* The most important anti-hacker products to use are anti-virus software, which scans regularly, and an ad blocker to stop unnecessary items making their way onto your desktop. We install Avast! at NSCAD.



* Actions that reduce risk

*Actions that reduce risk

Keep your security up to date

Be sure your anti-virus software is kept up-to-date when possible. Make sure you use the latest version of your web browser and be sure to install security patches and software updates once they are available.

Clear your browser history

* This is quite an important tip to use if you're going to be using the same device as someone else eg. your home computer or iPad. Many browsers keep a record of what you've searched for online, where you've been and the sites you may have visited. This information could be kept for a matter of days or weeks, and so without clearing the browsing history, it's easy for anyone in contact with the desktop to steal your online activity record.

* Actions that reduce risk

Why complex passwords are necessary

* Experts say it can take a hacker up to two years to crack a complex eight-character password. So use those numbers and capital letters and it will help!

* Actions that reduce risk

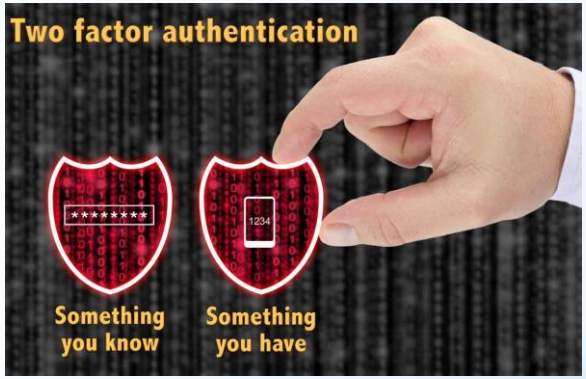
Never use the same password on all accounts

* The most important advice is to never use the same password twice. If one account is compromised, then all your accounts are compromised.

* Actions that reduce risk

Two Factor Authentication

* It is wise to set up two factor authentication (or 2FA) on all your important accounts. This is an extra layer of security that requires not only a password and username, but something else – something that you, and only you, have.



* Actions that reduce risk

Fabricate personal information when creating password security questions

* “Where were you born?” or “what’s your mother’s maiden name?” are two of the most common questions on websites to ensure your account will be safe from intruders in the future. These answers aren’t going to be the walls that will keep out any online attackers. This is because, if you’ve already divulged this information online, anyone could do some digging and find the answers they need. Don't be afraid to make up some of your information if you can.

* Actions that reduce risk

Never click on that link in an email

* Do not click on any links in any emails and always visit a website direct. Mouse over the links to see where the link points, copy and paste the link instead of clicking, and call the sender to verify the source.

* Actions that reduce risk

Keep emotions in check

* Most modern-day breaches contain an element of social engineering. An attacker often plays on human emotions. For example, asking you to click on a malicious link because it sounds like someone needs help or is in immediate danger.

* Actions that reduce risk

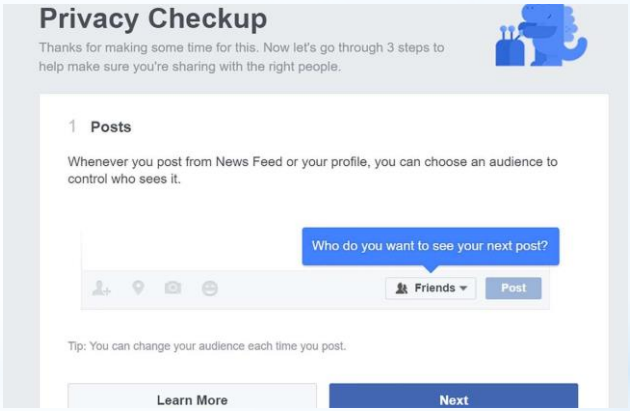
Have minimal information on your social media profiles

* The more personal information you share online the more your details are accessible to someone wanting to get their hands on it. Next time you're on your social media account, make sure the information you share is minimal. Your family and friends will already know your phone number, birth date and email address, so there is no need to divulge this information. If your privacy is important to you, don't give out your information freely. And, most importantly, don't tell people when you go away!

* Actions that reduce risk

Make sure your social network activity is private

* On your Facebook and Twitter accounts, head to the settings cog, usually in the top right corner of the screen. You are able to change all kinds of privacy settings, so only people you want to allow view your information can actually do so.



* Actions that reduce risk

*Actions that reduce risk

Avoid using public Wi-Fi

Do not do online banking or other sensitive activities on a public Wi-Fi network. Open networks can allow snooping, the network may already have compromised machines, or the hotspot itself could be malicious.

Don’t share unnecessarily

* Don’t share personal information with any network or site unless they need to know for a very important reason. For example, if you’re signing up to a public Wi-Fi hotspot it will ask for your name, date of birth and address. There’s no legal requirement, so make it up – keep your real details safe.

* Actions that reduce risk

Be wary of ‘free’ apps available

* It can be possible for hackers to download spyware onto your device through apps. Before installing, be sure to check the permissions on the apps to ensure they won’t store any unnecessary personal information.

* Actions that reduce risk

Privacy and Security

FOIPOP

* The Freedom of Information and Protection of Privacy Act
* There have been changes in the past couple years, mostly derived from real litigation
* Changes have mainly been aimed at tightening the act and expanding its coverage
* New copy on Computer Services website

Things Never to Put in Any Email

* Medical, dental or healthcare information
* Information regarding a possible violation of law
* Social insurance or welfare information
* Employment information (salaries)
* Educational information (grades)
* Personal financial information (net worth)
* Personal evaluations or character references
* Race, ethnicity or sexual orientation
* Religious or political beliefs or associations
* Name and address or name and phone number

* Privacy and Security

*Questions?