IS2109 Information Systems Security
Practical 4
Secure Web Browsing

1. Adware

a. Adwares is the one kind of unwanted software which supports advertisements. These softwares will automatically deliver advertisements during the program is running. Creators of adware include advertisements or help distribute other software to earn money. In many cases, ads may be within the software itself. Very common examples of adware include pop-up ads in websites and ads displayed while a program is running.

b. Companies integrate adwares into their softwares itself. This will load the advertisement when the particular program is running. These ad spaces are also bought by other companies to display theri ads. In some cases , we can't run the programs unless the ads are being displayed, we should disable our ad blockers to run the programs. Adwares also collect personal information and brower habits of users and sell those information to third parties.

c. Computer will slow down.
Ads are displayed
Will get many pop-up messages
Browser home page will change without out concern
Browser may crash
Unfamiliar icons and shortcuts display on the desktop.

d. Can use programs like *Malwarebytes for Windows, Malwarebytes for Mac, Malwarebytes for Android, Malwarebytes for Chromebook, and Malwarebytes for iOS*
Remove all malicious programs from PC

2.Credit Card Fraud

a. Credit card fraud happens when a person shares his credit card details with unfamiliar individuals and in unwanted online places or when the lost card gets into the criminal's hand. Also credit card skimming can occur. That means criminals make an illegal copy of a credit card using a device which can read and duplicate in the original credit card. Another type is phishing, criminals will send email to customers which looks like they come from a particular bank. And if we fill those details criminals will get our card details.

b. Should keep our card safe
Do not throw credit card billing statements directly into trash, those consider full credit card number
Avoid sharing your credit card information with others
Be safe while using credit online
Report to bank when card is stolen or lost
Review billing details regularly
Should have very strong passwords

c. <u>Safe email practises</u>
   - Should not ever send credit card details on email
   - Be aware when going for a purchase from a link which came in email
   - Limit public information, Attackers cannot target your employees if they don't know their email addresses.
   - Carefully check emails.
   - Beware links and attachments.
   - Hover over hyperlinks.
   - Never enter your password.

<u>precautions to prevent credit card fraud</u>
   - Be careful who you purchase goods and services from
   - Verify physical addresses and reputation
   - Utilize temporary credit card numbers
   - Never respond to requests for personal Information
   - Create complicated passwords
   - Safeguard your passwords and change them often

3.Browser Hijacking

a. Browser Hijacking is a form of unwanted software that modifies a web browser's settings without a user's permission.Browser hijacking software can do things with your browser that we didn't intend to do yourself.

b. Don't click attachments from unknown senders. Just as you might be suspicious of large, anonymous packages in the mail, don't open an email if you don't know the sender.

   Good antivirus software is always important in the fight against browser hijacking and making sure your device is kept safe.

   Browser and operating system (OS) updates are also important. Browser hijacking is all about looking for vulnerabilities in your OS and your browser. By making sure they are updated, you can ensure these vulnerabilities aren't found.

   Be aware before you download. Sounds obvious but take the time and read the small print.

   Use a digital security system like Clario. Our service is different to antivirus in that it monitors your browsing in real-time and works for you before the hijack occurs or is spotted.

4.Session Hijacking

a. Session Hijacking is also known as cookie hijacking. It is used to gain unauthorized access to information or services in a computer system. In this the user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out. The attack relies on the attacker's knowledge of your session cookie and specifically takes place when a session is started by logging into a service. This commonly takes place in browser sessions and web applications.

b. The two main types are
   - Application Layer Hijacking
   - Transport Layer Hijacking

c. The best way to prevent session hijacking is enabling the protection from the client side. So it must be done as a preventive measure to not let the session hijacking take place in the first place. The users should have efficient antivirus, anti-malware software, and should keep the software up to date.The use of fingerprint session or a particular face ID and configuring the http headers of the session for each time limit will stay as effective as against the intrusion when such hijacking occurs.

5.Spam & Phishing

A. spam is unsolicited bulk messages, that is, messages sent to multiple recipients who did not ask for them. The problems caused by spam are due to the combination of the unsolicited and bulk aspects; the quantity of unwanted messages swamps messaging systems and drowns out the messages that recipients do want.

B. Never give out or post your email address publicly.
Think before you click.
Do not reply to spam messages.
Download spam filtering tools and anti-virus software.
Avoid using your personal or business email address.

C. Phishing is one of the easiest forms of cyberattack for criminals to carry out, and one of the easiest to fall for. It's also one that can provide everything hackers need to ransack their targets' personal and work accounts.

D. Keep Informed About Phishing Techniques

New phishing scams are being developed all the time. Without staying on top of these new phishing techniques,we could inadvertently fall prey to one. Keep our eyes peeled for news about new phishing scams. By finding out about them as early as possible, you will be at much lower risk of getting snared by one. For IT administrators, ongoing security awareness training and simulated phishing for all users is highly recommended in keeping security top of mind throughout the organization.

Think Before You Click!

It’s fine to click on links when we’re on trusted sites. Clicking on links that appear in random emails and instant messages, however, isn’t such a smart move. Hover over links that you are unsure of before clicking on them.

Install an Anti-Phishing Toolbar

Most popular Internet browsers can be customized with anti-phishing toolbars. Such toolbars run quick checks on the sites that you are visiting and compare them to lists of known phishing sites. If you stumble upon a malicious site, the toolbar will alert you about it. This is just one more layer of protection against phishing scams, and it is completely free.

Verify a Site’s Security

It’s natural to be a little wary about supplying sensitive financial information online. As long as you are on a secure website, however, you shouldn’t run into any trouble. Before submitting any information, make sure the site’s URL begins with “https” and there should be a closed lock icon near the address bar.

Check Your Online Accounts Regularly

If we don't visit an online account for a while, someone could be having a field day with it. Even if you don't technically need to, check in with each of your online accounts on a regular basis. Get into the habit of changing your passwords regularly too.

Keep Your Browser Up to Date

Security patches are released for popular browsers all the time. They are released in response to the security loopholes that phishers and other hackers inevitably discover and exploit. If you typically ignore messages about updating your browsers, stop. The minute an update is available, download and install it.

Use Firewalls

High-quality firewalls act as buffers between you, your computer and outside intruders. You should use two different kinds: a desktop firewall and a network firewall. The first option is a type of software, and the second option is a type of hardware. When used together, they drastically reduce the odds of hackers and phishers infiltrating your computer or your network.

Never Give Out Personal Information

As a general rule, you should never share personal or financially sensitive information over the Internet. This rule spans all the way back to the days of America Online, when users had to be warned constantly due to the success of early phishing scams. When in doubt, go visit the main website of the company in question, get their number and give them a call.

Use Antivirus Software

There are plenty of reasons to use antivirus software. Special signatures that are included with antivirus software guard against known technology workarounds and loopholes. Just be sure to keep your software up to date.

References

https://clario.co/blog/live-secured/getting-rid-of-browser-hijacker/
https://www.internetsociety.org/resources/doc/2014/what-is-spam/
https://www.zdnet.com/article/what-is-phishing-how-to-protect-yourself-from-scam
https://www.phishing.org/10-ways-to-avoid-phishing-scams
https://channels.theinnovationenterprise.com/articles/7-ways-to-avoid-online-credit-card-

Group 07

Name	Index Number
R.M.D.K.B. Rajakaruna	18020641
W.H.M. Gunathilaka	18020275
S. Maayura	18020461
T. Athavan	18020097
T. Thushanthan	18020844