Technology Safety and Hacking

ELA AREA PUBLIC LIBRARY

*Hacking: to manipulate *a computer* skillfully, **especially** to gain unauthorized access to another system.* http://dictionary.reference.com/browse/hacking *or any technology

Who are the hackers?

+ / –

- Militaries and Governments – like the USA hacking the Iranian nuclear program centrifuges to destroy them, China hacking Google for trade secrets, North Korea hacking Sony because of *The Interview* movie. –

- Corporations – Google revenge-hacking China to investigate, for example. –

- Teenagers – From casually rebellious computer-savvy teens (sometimes called "script kiddies") to super-serious younger hackers. –

- Foreigners – Impoverished, desperate, and / or criminally greedy foreigners often try hacking. –

- Hackers – general hackers can use their skills to quickly make new legitimate software, crack other good software, or design their own malicious technologies (when being evil, called "black hat hackers"). –

- Security researchers – benign hackers, called "white hats", find and fix flaws. They use the same techniques as other hackers but for good. +

Why do they hack?

- Profit – even if only 1% of people fall for hacks, they can be very profitable. –

- For the "Lulz" – to laugh at the creators and users of vulnerable systems. –

- Activism/hacktivism – hacking that is done as a protest. ?

- Security – test systems to find flaws and eventually publish updates. +

How do they hack us? (they may use multiple of these methods)

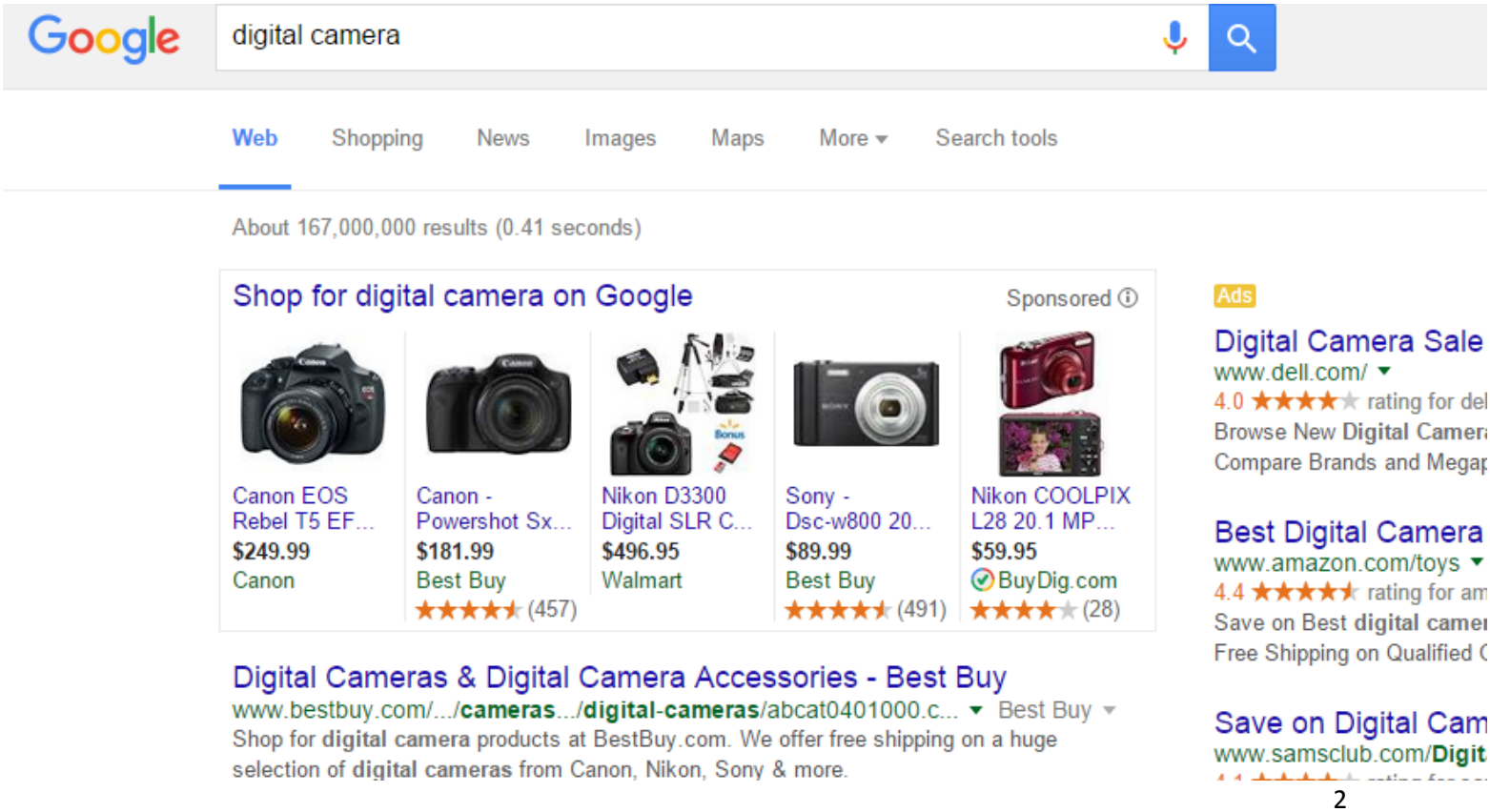
- Trojan horses – malicious computer programs that misrepresent themselves to appear useful, routine, interesting, or mandatory in order to persuade a victim to do something. https://en.wikipedia.org/wiki/Trojan_horse_(computing)

- Phishing – techniques used to gain personal information for identity theft etc. http://www.computerworld.com/article/2575156/security0/phishing.html

- Social engineering – manipulating people to give hackers access to their devices or reveal personal information. http://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

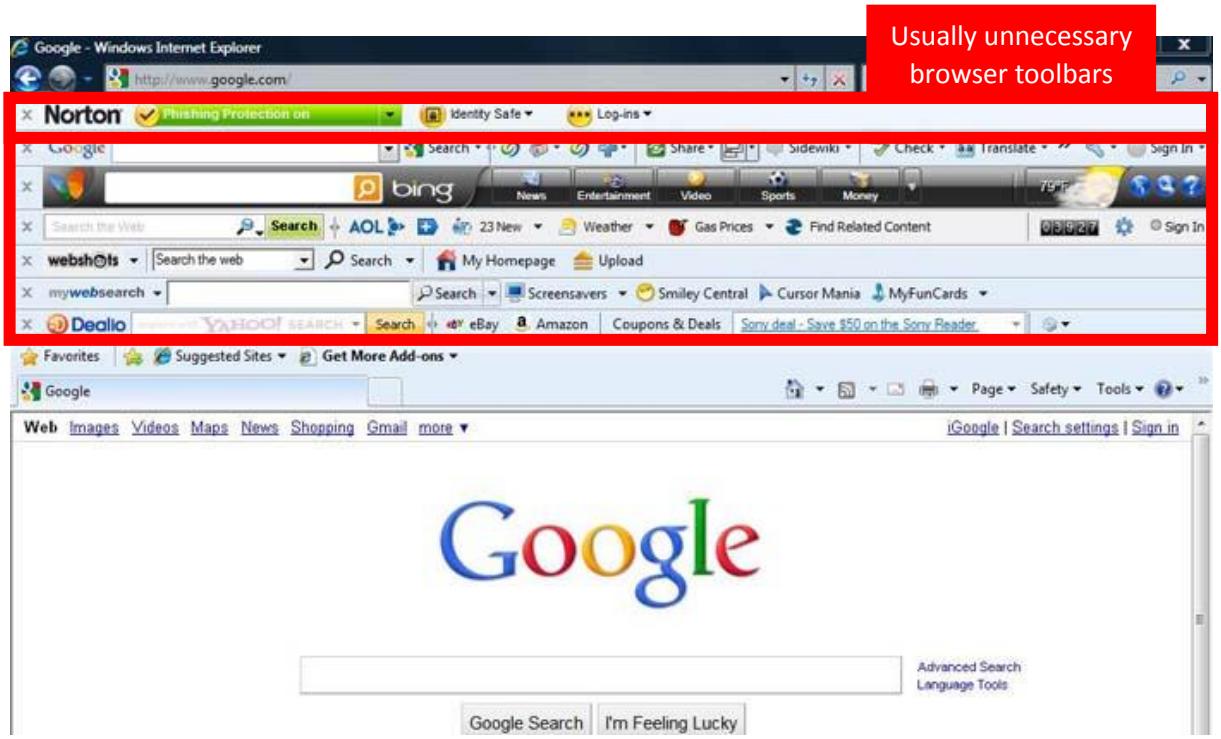
What specific threats are out there?

- Advertisements – unfortunately, ads often lead to illegitimate websites. Advertisements are usually marked “Ad”, “Advertisement”, “Sponsored”, “Promoted”, “From our partners,” “From [online advertising company name]”, “Recommended from [advertising partner company name]”. A lot of times

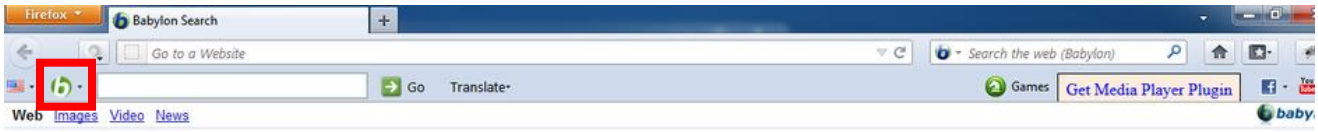


these labels are purposefully designed to be hard to see. Ads with pictures ("display" ads) tend to be more dangerous than text-only ads. Legit ads from reputable companies can also be infected by evil hackers in between the legitimate company and the site the ad appears on. **RISK:** High because almost all web pages have ads. Many ads are fine, but many are from shadier organizations. Avoiding clicking any ads at all is the safest strategy.

- Browser toolbars – **Web browser toolbars** are horizontal menus that legitimate and illegitimate sources offer to install to "improve" your browser. Some of these toolbars can actually help you with nifty additional tools. But others can change your search engine, home page, use your computer to send spam, and do other evil things. Malicious toolbars sometimes install themselves. Toolbars may also be installed into your web browser during the process of installing other applications. These toolbars waste space and the legitimate ones are gradually being phased out by most companies. Also, browser toolbars can slow down the speed of your Internet and your computer.
  RISK: Low if you stick to legitimate websites and avoid all browser toolbars.

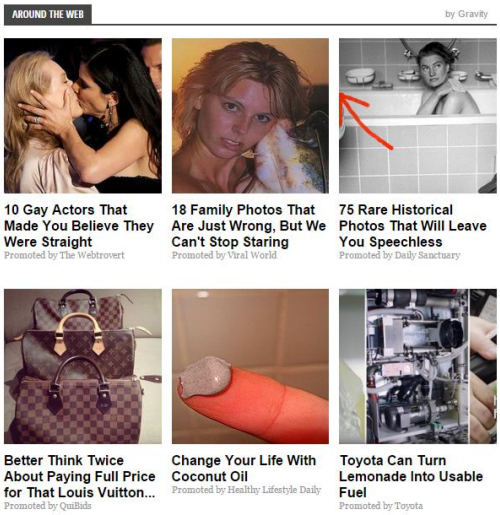


- Browser hijackers – Similar to browser toolbars, some infected websites and malicious programs sometimes hijack your web browser home page. They change your search engine to something that looks like Google but isn't, they generate pop-up advertisements, and do other evil things. Browser hijackers are not exactly viruses and tend to be fairly easy to remove using your web browsers settings or menus for **add-ons** and/or **plug-ins**, but they are malicious. *Pictured below: "Babylon" toolbar & browser hijacker*.
  RISK: Low if you stick to legitimate sites, avoid unnecessary or fraudulent plug-ins, and keep browsers up-to-date.

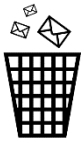


- Fake Antivirus ("scareware") and malicious alerts – hackers sometimes install software on machines that claims to be your antivirus software and asks for money. Some infected or malicious websites may not allow you to close them or may threaten you with multiple or repeated alerts that you're being attacked, or have been hacked, etc. They often tell you to go to a website or call a support number. These are scams. The real "hack" these hackers accomplish is when you give them further access to your system, etc. The real hack is preying on your fear or ignorance. This is one of the most common tactics of hackers these days.
  RISK: low if you stick to legit sites and avoid…

- Clickbait – clickbait is news articles or links that are written in such a way to get anyone interested. They prey on our natural curiosity. Don't click them, even if you see them in social media like Facebook. They often are accompanied with salacious pictures as well. Although the sites that use clickbait are not necessarily any kind of threat, they do tend to be seedier websites which have a higher likelihood of being insecure/malicious. *Buzzfeed: "17 Moments Anyone Who's Been To A College Party Deeply Understands."*



RISK: high if you click, low if you don't, low if you stick to legitimate websites.



- Spam Emails – are a common method of hackers. Popular email services filter out most spam. The best thing to do is to delete any spam messages that get through without opening them. Any links or attachments in spam emails or emails from sources with which you're unfamiliar should be treated with caution. A specific type of spam email threat is a **419 scam**. The scammers tell you that if you give them a little bit of money they'll be able to access some long lost bank account worth millions and they'll give you a cut. If you give them money, you'll never see your money back. Don't respond to these messages, simply delete them. Linked groups of hacked computers called **botnets** are often responsible for spam. Chain letters, forwards, and emailed jokes can also be dangerous if any of the previous recipients before you had been hacked. **RISK:** High if you do anything other than delete spam.

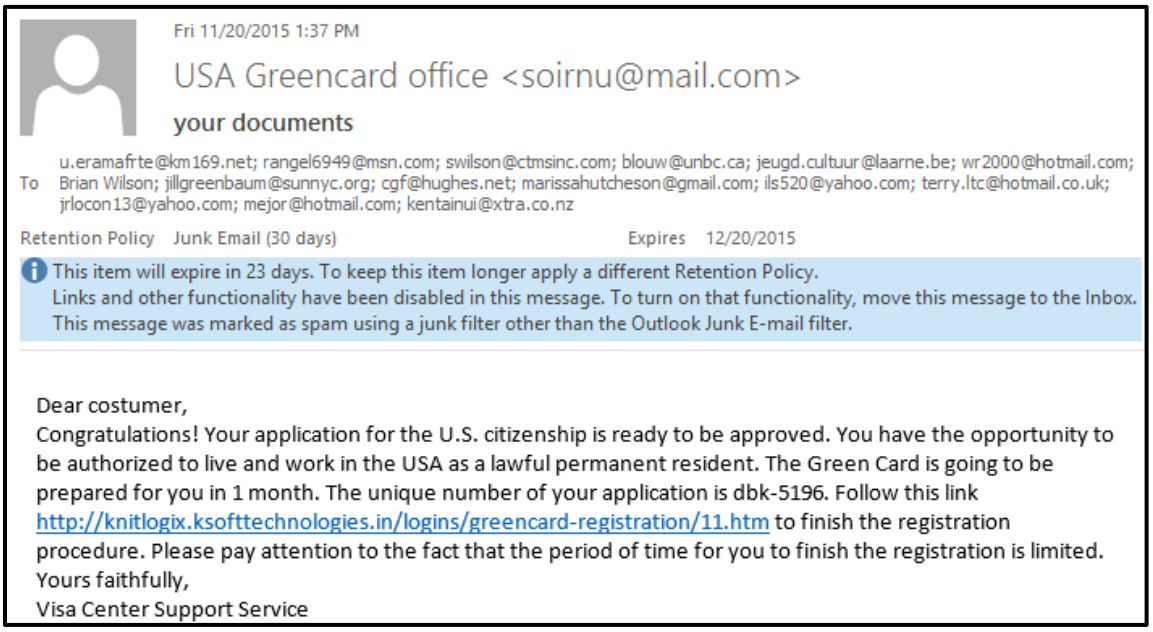
GOOGLE ANNIVERSARY WINNING NOTIFICATION

We wish to congratulate you on this note, for being part of our selected winners in our just concluded internal promotion draw this year, this promotion was set-up to encourage the active users of the Google search engine and the Google ancillary services.

Hence we do believe with your winning prize, you will continue to be an active patronage to the Google search engine and services. Google is now the biggest search engine worldwide and in an effort to make sure that it remains the most widely used search engine, we ran an online e-mail beta draw which your email address won Nine Hundred and Fifty Thousand Great British Pounds Sterling (J950,000.00). We wish to formally announce to you that you have successfully passed the requirements, statutory obligations, verifications, validations and satisfactory report Test conducted for all online winners.

A winning check will be issued in your name by Google Promotion Award; for the sum of Nine Hundred and Fifty Thousand Great British Pounds Sterling (J950,000.00) and also a certificate of prize claims will be sent alongside your winning check cashable at any bank.

You are advised to contact the assigned Google Program Administrator/Coordinator with the following details to avoid unnecessary delay and complications:



Fri 11/20/2015 1:37 PM

USA Greencard office <soirnu@mail.com>

your documents

To u.eramafrte@km169.net; rangel6949@msn.com; swilson@ctmsinc.com; blouw@unbc.ca; jeugd.cultuur@laarne.be; wr2000@hotmail.com; Brian Wilson; jillgreenbaum@sunnyc.org; cgf@hughes.net; marissahutcheson@gmail.com; ils520@yahoo.com; terry.ltc@hotmail.co.uk; jrlocon13@yahoo.com; mejor@hotmail.com; kentainui@xtra.co.nz

Retention Policy Junk Email (30 days) Expires 12/20/2015

This item will expire in 23 days. To keep this item longer apply a different Retention Policy.
Links and other functionality have been disabled in this message. To turn on that functionality, move this message to the Inbox.
This message was marked as spam using a junk filter other than the Outlook Junk E-mail filter.

Dear costumer,
Congratulations! Your application for the U.S. citizenship is ready to be approved. You have the opportunity to be authorized to live and work in the USA as a lawful permanent resident. The Green Card is going to be prepared for you in 1 month. The unique number of your application is dbk-5196. Follow this link http://knitlogix.ksofttechnologies.in/logins/greencard-registration/11.htm to finish the registration procedure. Please pay attention to the fact that the period of time for you to finish the registration is limited.
Yours faithfully,
Visa Center Support Service

There are tons of problems with this spam message:

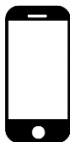
- soirnu@mail.com is not an official US government email address.
- "USA Greencard office" is the incorrect organization name.
- Lower cased "your documents" subject is highly unprofessional for the US government.
- Our government would use Bcc: not To: for sending one message to many people.
- "Customer" is not a very specific salutation. The government usually knows your name.
- The body text of the message was irrelevant and unsolicited by the recipient of this email.
- The link ends in ".in" instead of the US governments ".gov" domain.

- Cold calls – have you ever received a call from "Microsoft Security", "Computer Security", "Member Services", the "IRS", or "Card Services"? These unsolicited calls are scams and likely violate the Do-Not-Call Implementation Act of 2003. The credit card-related calls simply want to steal your credit card number. Use your caller ID to screen calls and ignore those from people and organizations you don't know. If you respond to the computer-related calls, they will instruct you to give them remote access to your computer. Once they have access, they will likely install a fake antivirus program and demand money to "fix" the "problem" *they created!* **RISK:** High if you do anything other than hang up on these crooks immediately. Zero risk if you simply hang up.

- Popups – are extra windows usually created by webpages that pop either over (**popups**) or under (**popunders**) the page you're currently on. They can be 100% benign, they can be something you actually need and want to click, they can be ads, or they can be malicious alerts. Most web browsers try to block popups automatically. You can manually override your popup blocker if a legitimate page you're on uses popups that you need. **RISK:** Low if you close popups as soon as you discover them and leave your web browser popup blocker turned on.

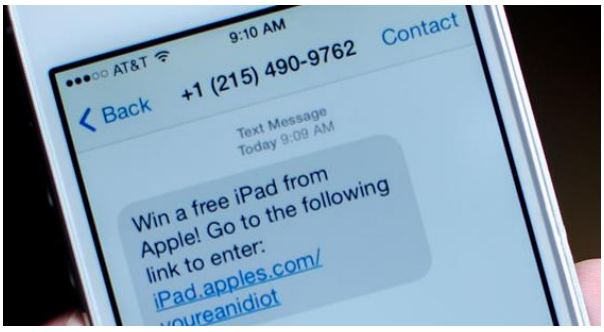
- Downloads – The internet is famous for "routing around attempts at censorship". Theoretically everything is available somewhere. There's a temptation to try to get everything for free, hunt around to download whatever you're looking for from somewhere. Sometimes downloads can be threats.
  - Program installer files usually end in .EXE
  - Free software pages have many download buttons, most ads, only one legitimate.
  - If you're downloading other types of files, the file extension will vary. PDF documents should be .PDF. Word text documents should be .DOCX or .DOC.
  - Be wary of any files that have endings that look like this .PDF.EXE. They're trying to trick you into thinking the file is a benign PDF when really it's a potentially dangerous .EXE executable file that can make changes to your computer.
  - Bit torrents are files simultaneously downloaded from multiple people who use special file sharing software. They are very risky to download.

  RISK: Legitimate sources-low. Free, illegal, pirate, and torrent sites-very high.



- Spam text messages – Spam text ads are likely illegal, but that doesn't stop crooks. Use the contacts feature of your phone to enter in the people and organizations you actually know and use, and then disregard other calls. Do not respond to unsolicited spam texts. Do not click on any links in spam texts. Delete the spam text messages and block the contact if possible.

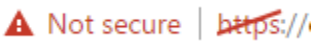
  RISK: Low as long as you ignore them.



- Ransomware – Ransomware hacks are increasing in prevalence. A hacker somehow gets access to a flash drive or your whole computer. They then encrypt whatever they control. In exchange for a (usually bitcoin) ransom payment, the hacker will allow you back in. **RISK:** Increasing as more hackers are turning to ransomware. Keep your antivirus software up-to-date and make sure to have backups of important info. Reformat or simply don't trust unknown flash drives.

What you can do

- Identity theft – The end result of some hacks is hackers having access to personal information such as your credit card number, bank account info, etc. The hackers will then do evil stuff such as withdrawing money, over drafting, buying things online. To try to prevent identity theft, only do business online with reputable companies like major retailers, Amazon etc. Smaller websites are more likely to have insecure payment systems. Look for web addresses that start with **https://**. The **s** in **https://** stands for **secure** using a security technology called **SSL**. SSL isn't perfect, but helps at least secure your connection to a website. A ~~crossed through https://~~ means SSL didn't work. **PayPal** and **Bitcoin** are alternative online payment methods—most websites support standard credit cards. Track your credit card statements carefully. Dispute any charges with your credit card company. Request a new credit card. It will have a new number and 3- or 4-digit **security code**. The new **chip and PIN** credit cards are more secure than traditional swipe-only cards. Other options including **Apple Pay**, **Google Android Pay**, and **Samsung Pay** also add extra layers of security (along with being more complex to set up unfortunately). After you've received a new credit card, log in to accounts and remove the old or compromised credit card(s) from your account information and add the new one.



After having your identity stolen, you may want to check a credit report. The three major credit rating agencies, **Experian**, **Equifax**, and **TransUnion** generate these reports. You can get at least one report free each year.

For more info or to dispute report items see www.annualcreditreport.com or contact:

Equifax
PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

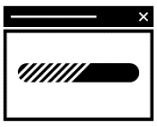
Experian
Consumer Fraud Assistance
PO Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
Fraud Victim Assistance Division
PO Box 6790
Fullerton, CA 92834
1-800-680-7289
www.transunion.com

- Antivirus software – We highly recommend that you install antivirus and antispyware software on your computer, especially if you have a Microsoft Windows operating system. Although not recommended, most Apple macOS users go without antivirus software without problems. Antivirus and -spy software can block potential hackers from compromising your system. They aren't perfect, though. Antivirus programs also typically do scans of files on your computer to make sure they haven't been covertly infected. Typically these programs do either quick scans of some of your files or full scans of everything on your computer. If your antivirus program is doing a full scan, make sure to leave your computer on for a while. Some antivirus software is available for free, while other antivirus software is sold on a subscription basis.

Some reputable antivirus company logos (left to right): Microsoft Windows Defender, McAfee, AVG, Trend Micro, Norton, Avast, Kaspersky, Webroot

- Firewalls – a firewall is a computer security feature that prevents unauthorized access to your computer. Rather than addressing specific threats like antivirus, firewalls block general threats, whole types of threats. Most operating systems have software firewalls enabled by default. We recommend leaving firewalls turned on.

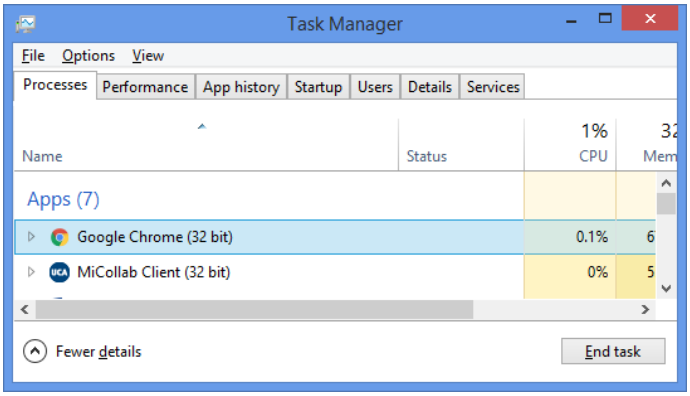


- Updates – One of the best things you can do to keep your technology secure is make sure it is up-to-date. These days, most programs let you know when the version you're using is out-of-date and prompt you to download and install the latest version. This is good and bad because it's good to keep software up-to-date, but software makers tend to make updates very regularly. Keeping your tablets and phones up-to-date is trickier because the files required to update those devices tend to be very large. Plug devices in while updating. Sometimes updates themselves introduce new issues. Release notes often explain the purpose of an update. A few programs that seem to be asking to update all of the time:
  - **Adobe PDF reader** – for viewing PDF documents
  - **Adobe Flash** – helps make online games and video players like YouTube work
  - **Adobe Updater** – silly program that helps keep Adobe PDF and Flash up-to-date
  - **Firefox** (by Mozilla) – free web browser (like Internet Explorer or Google Chrome)

During the process of updating, some of these legitimate programs will give you offers for free downloads such as web browser toolbars (see above) or other software. The vast majority of this software is not anything you need. We recommend unchecking or otherwise saying no to these offers. You only want Flash, Firefox, Java, etc. not the other junk.

- Use secure passwords – unfortunately, this is a very difficult task. A lot of online accounts force you to create very insecure passwords. Check your password at https://howsecureismypassword.net/ . A secure password typically:
  - Is fairly long with a few #s 1234567890 and UPPERCASE and lowercase letters
  - Has symbols!@#$%^&*()[]{}.-_ but watch account creation pages carefully, as some (more insecure) services ban using certain symbols in passwords
  - Memorable, yet unique
  - You may need to write down passwords and keep them in a physical folder
  - Consider letting browsers or dedicated password managers remember yours

- Task manager – if popups won't close or a program is misbehaving, you can use the Windows **Task Manager** to manually quit out of programs. Using the keyboard shortcut Ctrl+Shift+Esc, you can pull up the Task manager. This is a part of the Ctrl+Alt+Del program which allows you to manually quit out of applications. Once you have task manager open, click into Processes, then single left click on the name of the program that's being suspicious/causing problems. Then, click **End Task** in the lower right corner and the application will close. (Mac equivalent of Task manager: **Force Quit** in the **Apple Menu**.)



- Enable two-factor authentication – For added security, some services require two steps to log in to an account. Step 1) Like usual, you have to correctly type in your username and password. Step 2) After that, you also have to type in a numeric code the service text messages to your cell phone.

Distinguish between legitimate content and spams

- Scams
  - Unsolicited (spam emails/phone calls) gifts, awards, too good to be true
  - Pushy
  - Threatening
  - Malicious looking links
  - Impersonation
  - Bad grammar
  - Advertising
  - Difficult to close
  - Claim to be family
- Not scams
  - Solicited (responding directly to something you did)
  - Legitimate or known sources

- Secure your mobile phone – our mobile phones have tons of personal information on them today: emails, pictures, videos, credit card(s), bank account info, Facebook, etc. A lost or hacked phone can be devastating.
  - If your phone has a finger print reader, set that up to be more secure. You can enable a passcode or password as well. Devices can be set to lock themselves after a certain number of incorrect passcode or finger print entry attempts.
  - Don't lose your device! But if you do, Apple's "Find my iPhone" and Google Android's "Find My Device" can help you locate and/or potentially disable lost devices as well. Your phone company may also be able to help.
  - If you don't use it, turn off BlueTooth to prevent unwanted local connections.
  - Download apps only from Android's Google Play store, or Apple iOS App Store.
  - Update your device regularly.
  - Don't "root" or "jailbreak" your device.
  - Ignore calls and voicemail from unfamiliar numbers, unfamiliar zip codes. Google unfamiliar phone numbers before calling back. Block if possible.
  - Back up your device, especially photos. Services like Google Photos, Dropbox, Microsoft OneDrive, and Apple iCloud and many more make this fairly easy.
  - Keep your device in your front pocket. (Back pockets are easier to pick!)

- Secure web cameras and ports – device cameras or open plugs are vulnerabilities you can protect against. Web cameras typically display a light nearby when they are being used. Computer plugs tend to automatically access anything that is plugged in to them. If you are at all concerned about a web camera, simply cover it up. Covers or locks can also be purchased for plugs.

REVIEW / Standard responses to some common threats:

Advertisements – ignore, don't click
Browser toolbars and extensions – don't let them install or uninstall
Browser hijackers – remove/uninstall and reset your homepage
Fake antivirus and malicious alerts – close if possible, otherwise power off
Clickbait – don't click
Cold calls – hang up
Popups – close them
Risky downloads – avoid illegitimate sources, don't click "download" ads
Phone spam – delete texts, block the sender if possible

- What to do after you've been hacked – some general advice

Log in and then immediately reset your password

  - Manually go directly to the site that was hacked, rather than clicking thru from an email. If you set up security questions (like Q: What's your favorite animal? A: Platypus), make sure the hacker didn't change them, change them yourself.
  - It's also advisable to change passwords for other services you use, just in case.

Or use account recovery tools:

  - Apple https://iforgot.apple.com/iForgot/iForgot.html
  - Facebook https://www.facebook.com/help/231208473756221, https://www.facebook.com/help/131719720300233
  - Google https://www.google.com/accounts/recovery
  - Microsoft https://account.live.com/acsr?rollrs=04
  - Twitter https://support.twitter.com/forms/hacked
  - Yahoo https://edit.yahoo.com/forgotroot/
  - Many of these tools use two factor authentication to be secure: they require you to enter in 1) the email address of the account you can't access, AND 2) type in a code they send to your mobile phone

Install or update your antivirus

- If you didn't have antivirus software and were hacked, you probably should've had it. Don't Google "free antivirus software". Install and set up a legitimate antivirus package such as Microsoft Windows Defender, McAfee, AVG, Norton Antivirus, or Trend Micro.

Uninstall any programs or browser extensions that may have been installed

- Sometimes viruses install programs or web browser extensions on your computer. They can be incredibly difficult to remove, but you definitely need to get rid of them, otherwise the hacker still has access to your system.

Make sure your web browser, plug-ins, and operating system are up-to-date

- Vulnerabilities caused by simple program bugs are often how hackers get in.
- Make sure web browsers are up-to-date. (Chrome, Firefox update frequently, IE doesn't.)
- Reset your web browser home page if the hacker changed it.
- Update any plugins you have installed such as Adobe Flash or Java as well.
- Update your entire computer as well – bugs there can let hackers in too.

Let some certain people know you were hacked

- Don't send a message to absolutely everyone, but you could contact a few important friends to let them know or post a status update on Facebook if you've been hacked there.

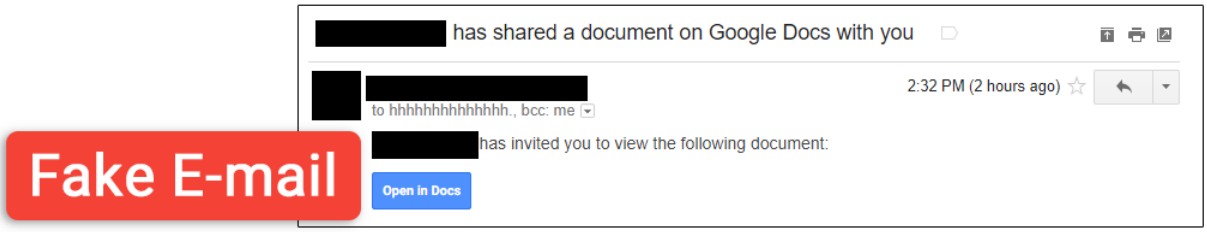
Monitor for suspicious activity

- Social media: Is there anything there you didn't mean to post?
- Is your credit card being used fraudulently? If so, request a new card. It should have a new number. Update account info on websites you purchase items on.
- Check your sent email folder. Did you send everything out?
- Has anything changed in your account such as your email signature?

Step-by-step analysis of one Phishing attack

On May 3rd, 2016 a major phishing attack hit Google Docs. A hacker claimed to be sharing Google Documents and emailed a link to people. It linked to a deceptive app that hijacked anyone who clicked through two steps. Here's how it worked:

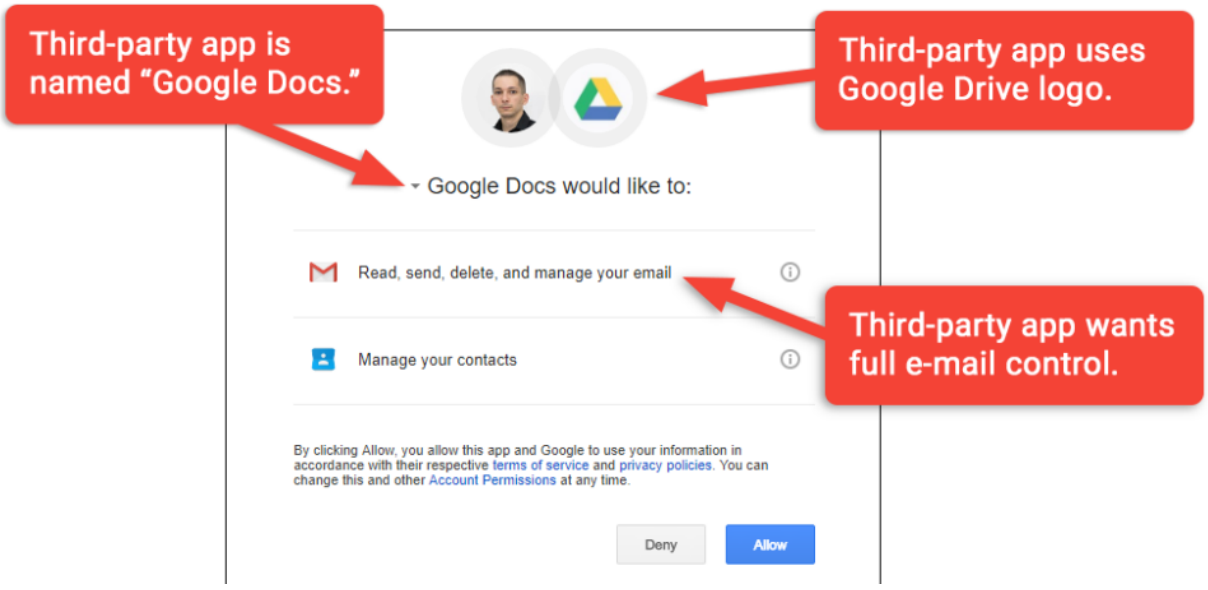
Step 1: Receive a Phishing email

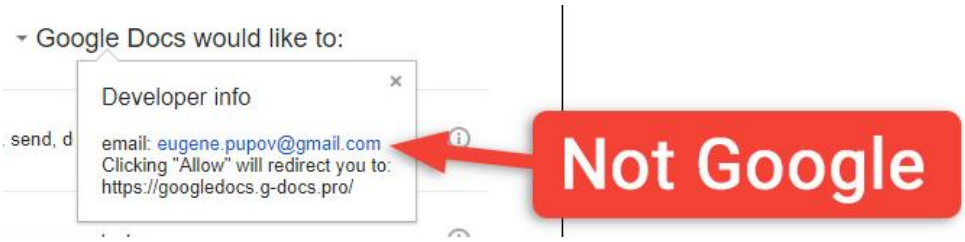


The "**Open in Docs**" button is almost exactly the same as the real one, BUT:

- BCC: Cloud services typically don't BCC sharing requests. BCC has its purposes, here it is used to automate sending the emails and to deceive you into believing you were the only intended recipient – you weren't.
- FROM ADDRESS: Does hhhhhhhhhhhhhh@mailinator.com sound like the address Google Docs would send you an email from? No, it doesn't.
- FROM DOMAIN: @mailinator.com is a disposable email service. Mailinator addresses cannot send email. They can only receive email. The hacker attempts to make this look like a normal email when it's anything but.

Step 2: Click the Fraudulent "Open in Docs" link





The "**Open in Docs**" link takes you to a legitimate screen of an application asking to be able to interact with your Google account. But this "app":

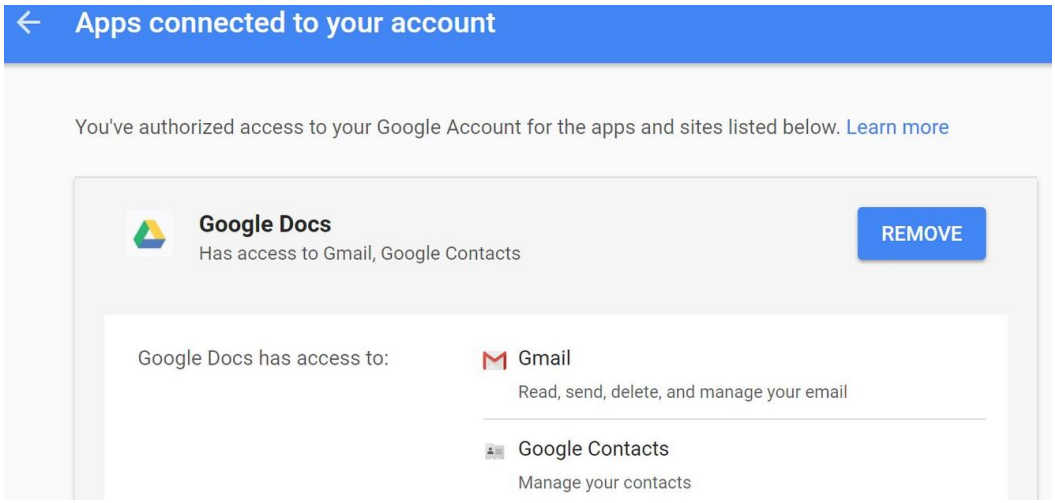
- Is calling itself "**Google Docs**". 3rd party applications interacting with and extending Google services shouldn't have the same names as Google services. That's copyright infringement. Apps should have unique names!
- The app's picture is the Google Docs logo. Again: 3rd party software should not be branded exactly the same as Google's 1st party (its own) software. Legitimate 3rd party applications should have their own branding.
- The developer info gives everything away.
  - The developer is some random "**eugene.pupov@gmail.com**" which is obviously not Google. The hacker is hoping you won't click into the dropdown menu that revealed this information. The Pupov account itself is likely a disposable account created only for this attack.
  - The developer web address **https://googledocs.g-docs.pro/** is not Google. Google addresses will end in something.google.com , not .pro. The rest of the web address is designed to *look* like a legitimate Google website, but obviously is not one.

Step 3: Exploit

- Look what the application developer is asking to do for you:
  read email, send email, delete email, and manage contacts.
  - Combined, these settings allow the developer to automatically:
    - Send emails to all of your contacts to spread further,
    - Delete those messages after they're sent so you can't detect it, AND
    - Export information from your email and contacts to use later.
- Overall, this is a nasty hack. Thankfully, Google has taken steps to decrease the likelihood of attacks like this in the future.

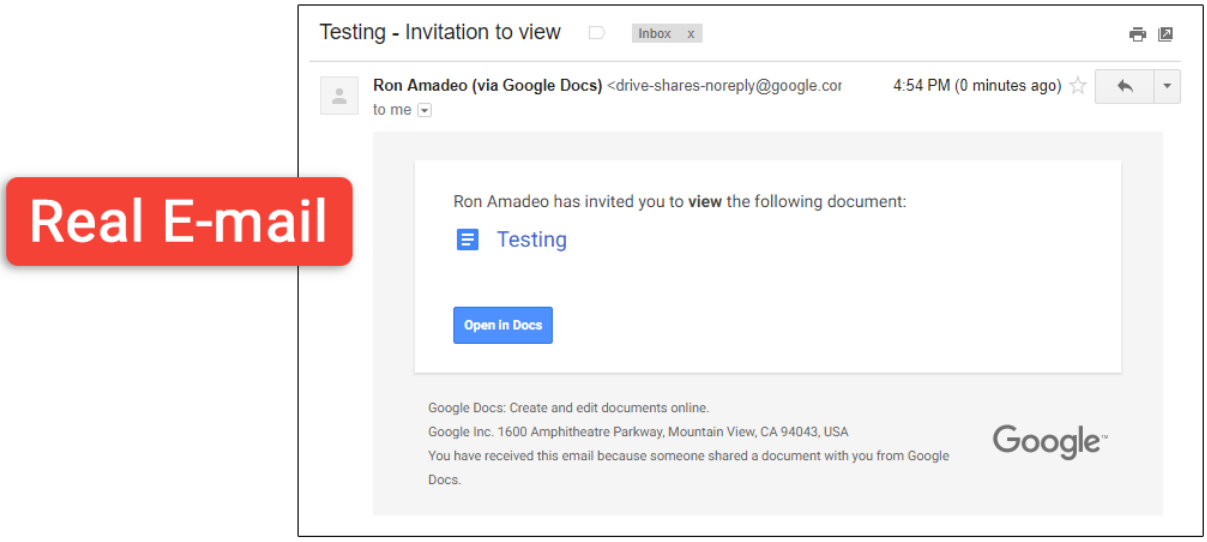
Step 4: Removing permissions from the developer

- Going about undoing a hack is different in each situation, but in this case:
  - Go to your Google permissions page: https://myaccount.google.com/permissions
  - There, find the app and revoke its access by clicking **REMOVE**.



  - (Google has likely automatically done this for all victims of this attack.)

Here's what a legitimate Google Docs sharing request looks like:



More information on this specific phishing attack:

https://en.wikipedia.org/wiki/Google_Docs,_Sheets_and_Slides#2017_phishing_incident

Specific examples and links:

Phishing Example of Google Docs attack of 5/3/2017: https://arstechnica.com/security/2017/05/dont-trust-oauth-why-the-google-docs-worm-was-so-convincing/
San José Public Library Privacy Lab: https://www.sjpl.org/privacy
Government hacking: http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0
Corporate hacking: http://www.nytimes.com/2010/01/15/world/asia/15diplo.html
Teenage hacking: https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/
General/other hackers: http://www.bloomberg.com/features/2015-george-hotz-self-driving-car/
Spam emails: http://imgur.com/a/MzzdU
Cold calls: https://www.youtube.com/watch?v=Rn5sBDwmZ5s
Pop-ups: http://www.theatlantic.com/technology/archive/2014/08/advertising-is-the-internets-original-sin/376041/
Downloads: http://xkcd.com/1247 , http://www.howtogeek.com/168691/how-to-avoid-installing-junk-programs-when-downloading-free-software/ , http://www.consumerreports.org/cro/2014/02/how-to-avoid-installing-software-you-don-t-want/index.htm
Spam texts: http://www.popsugar.com/tech/How-Block-Number-iPhone-31863584
Passwords: https://xkcd.com/936/ , https://howsecureismypassword.net/
National Do Not Call Registry: https://www.donotcall.gov/
FBI Internet Crime Complaint Center: https://www.ic3.gov/default.aspx
FTC technology safety videos: https://www.youtube.com/user/FTCvideos

Recommended Additional Resources:

Other technology classes
Go to http://www.eapl.org/events to view and signup for other computer classes.

Class handouts
Go to http://eapl.org/events/computer-programs/class-handouts to download copies of class handouts and exercise files.

Librarian and computer aide assistance
We are glad to help you out at the second floor reference desk as best we can while helping others.

Help appointments
Ela Library cardholders can schedule one-on-one appointments with librarians for further help. We can help with our Digital Media Labs or with general technology questions in our areas of expertise. Appointments last up to one hour. Paper appointment request forms are available at the 2nd floor reference desk. You can also request appointments online:

- Go here http://www.eapl.org/DMLhelp to sign up for a Digital Media Lab appointment.
- Go here http://www.eapl.org/one-one-technology-help-appointment-request to request a general tech help appointment.

Tech Tutoring
The last Wednesday of some months, a tech savvy librarian is available for six 30 minute tech tutoring appointments. Bring a list of questions and we'll help with as many as possible. Limit one tutoring appointment per month per patron. First registered first served, no library card required. Go to http://www.eapl.org/events to register for a session.

Databases
The Library offers card holders access to many premium databases. These include two which can help you learn more about technology.

- Gale Courses offers a wide range of highly interactive, instructor led courses that you can take entirely online. As an Ela Area Public Library card holder in good standing, you are entitled to these courses at no cost. Courses run for six weeks and new session begin every month.
- Lynda.com offers technology training with over 20,000 training videos on over 300 topics with exercise files included. The Library pays for you card holders in good standing to access this resource, however you will be required to create a free account. **Please remember to log out when you are finished.*

Access both of these databases from the library Research page: http://www.eapl.org/resources

Books
A few books in the library collection related to this topic are:

- **Ransomware: Defending Against Digital Extortion** by Allan Liska & Timothy Gallo
  Call Number: 005.8 LIS
- **Defeating the hacker: a non-technical guide to computer security** by Robert Schifreen
  Call Number: 005.8 SCH

Free online tech training websites
http://www.gcflearnfree.org/ , https://techboomers.com/ , http://digitallearn.org/

Computer Class Evaluation

Class Title: Technology Safety and Hacking Date: 8/15/2017

In terms of your skill with computers, how do you consider yourself?

□ Absolute Beginner (no or little experience with computers, NOT yet comfortable using a mouse and keyboard)
□ Beginner
□ Intermediate
□ Advanced

In terms of your skill in securing your computer from hackers, how do you consider yourself?

□ Absolute Beginner (no experience)
□ Beginner (some experience, but not comfortable using)
□ Intermediate (some experience, comfortable with the basics)
□ Intermediate/Advanced (experienced with basic and intermediate functions, but require training on advanced functions)

How much do you feel that you learned?

□ I learned a lot
□ I learned some
□ I didn't learn much
□ I learned nothing

How did you perceive the pace of the class?

□ Too Fast
□ Just Right
□ Too Slow

Were the handouts helpful?

□ Yes □ No If no, why not?

What did you like most about the class?

What did you like least about the class?

What other topics would you like to see in a future computer class?

How do you normally find out about library computer classes?

□ Footnotes (Library Newsletter)
□ Library Website
□ Other _____

If you're not an Ela Library card holder, where is your home library?

Any additional comments: