

HACKED!

SYDNEY BECKMAN
PROFESSOR OF LAW

SYDNEY.BECKMAN@LMUNET.EDU

The cybersecurity arena (both threats and defenses) is one that is constantly changing. Because everyone's needs, hardware and software configurations, and budgets are different, it is virtually impossible to make a recommendation as to any particular solution. The lists below offer a starting point to review popular options that may be available. I try to stay fairly up to date with regard to both current threats and methods to avoid them. Feel free to reach out to me and I will try to respond to any questions.

ANTIVIRUS SOFTWARE

Two important point to consider with regard to anti-virus software. First, no one particular piece of software has historically been able to protect against all threats. So, no matter how effective your software is, you should always proceed with caution. Second, do not think that more is better. It is generally recommended against installing more than one anti-virus software as serious conflicts may (and almost always will) arise leading to improper functionality of your PC. In any given year, or month for that matter, one may function better than another. Also, there are many options not listed below. I have generally selected some of the most popular ones. Bottom line, pick one.

Most antivirus software offers versions for both the PC and Mac. Also, some offer free versions. There are usually some cons related to the free version.

[Avast!](#)
[Avira](#)
[AVG](#)
[BitDefender](#)
[Kapersky](#)
[McAfee](#)
[Norton](#)
[Windows Defender](#)

CLOUD-BASED BACKUP

[Acronis](#)
[Backblaze](#)
[Carbonite](#)
[DropBox](#)
[Google Drive](#)
[iCloud](#)
[iDrive](#)
[OneDrive](#)

SOFTWARE-BASED BACKUP

[Acronis True Image](#)
[AOMEI Backupper](#)
[Cloudberry Backup](#)
[EaseUS ToDo Backup](#)
[ShadowMaker Pro](#)

EXTERNAL STORAGE DEVICES

Options for external storage devices are plentiful. Personally, I prefer a physical device with which to backup my data. That is simply my personal choice. There are advantages and disadvantages. Remember that all external devices are subject to loss, theft, destruction and failure. I recommend always having two backups and keeping them in separate physical locations.

Fundamentally you have three types of external backup devices: hard drives, solid state drives (SSDs) and flash drives (which are basically a smaller version of a solid state drive). The two largest manufactures of hard drives are Western Digital and Seagate. Much like Ford and Chevrolet, users take sides. I fall on the Western Digital side. Studies have been done which reflect that Seagate hard drives are much more prone to failure than Western Digital drives. My anecdotal experience mirrors those findings. Nevertheless, you will find people who swear by Seagate drives.

External hard drives come in many different sizes. Examine how much storage you currently use, add at least 30% to that number and purchase a hard drive that had that number as a minimum. Four terabyte hard drives cost roughly \$100 these days.

Links for purchase change rapidly. You can frequently find excellent deals on hard drives by searching on Amazon's website. You can search by brand, size, and numerous other options including color.

Solid State Drives are finally becoming affordable as options for external storage. They come in various sizes and costs. You can easily purchase 512GB SSDs for less than \$100. SSDs have a few advantages over external hard drives. They are smaller (much smaller); they have no moving parts which means they are both more durable and less likely to fail and they are significantly faster. I'm talking Superman fast compared to external hard drives.

Flash drives are like miniature SSDs both in size, capacity and cost. These have come way down in cost in recent years. You can find 64GB flash drives for less than \$10 and 128GB for less than \$20. Like SSDs these can be very fast. However, be aware that they are usually speed rated and inexpensive ones may be on the slow side. Also, because they are small, they are usually less durable. I have seen more than one broken because of accidentally being stepped on or chewed by a dog.

Bottom line, always buy a storage device that is larger than you need.

CAMERA COVERS / MICROPHONE MUTE

Although (statistically speaking) hacking into one's camera or microphone is relatively rare. Nevertheless, more and more people cover their cameras with sticky note, tape, et cetera. As to your camera, these methods work as well as anything. Unfortunately, these solutions must be reapplied if you actually sue your camera and aesthetically speaking they are not particularly attractive. Fortunately, camera covers are very cheap and have functional slides that can be opened and closed. Here is an example:

[Camera cover on Amazon](#)

Just as with cameras, there is the possibility for nefarious types to hack into a computer's microphone. As you know, you can plug in an external microphone. Small, non-working, devices can be used to plug into the external microphone ports which effectively "mute" the mic thereby preventing the hacking of the microphone. Here is an example of one of those:

[Microphone Blockers](#)

You will find many, many examples of camera covers and microphone blockers on Amazon (and other places).

IOS v. (PC/MAC/ANDROID)

I was asked about security as it relates to attachments. Attachments frequently are the source of malware or other cyberattacks which impact users. The common advice is not to open an attachment that comes from a source you don't trust. The problem is that cybercriminals are adept at spoofing (faking) the source of email and other communication. This means that an email that you think you are getting from your mom or boss might be coming from someone else.

My advice is to always use antivirus software to scan an attachment before you open it. If you don't have that option, then open the attachment on an iPhone or iPad. Why? Without boring you with the details, it is a much safer option than Android or even your PC. The way iDevices handle apps, makes it virtually impossible for a virus to infect your iPhone or iPad. For those that are interested, it is called sandboxing. The apps have virtual walls between them which, absent consent from Apple, prohibits one app from talking to the other. Some people find this annoying as it limits certain functionality. But the trade-off is heightened security.

AALS Technology Section Webinar Series

Hacked!
An Examination of Cyber-Threats
and Techniques to Thwart Them

June 26, 2019

AALS Technology Section Webinar Series

Welcome & Introductions

April Dawson
Professor, North Carolina
Central University School
of Law
Chair, Webinar Committee,
AALS Section on
Technology, Law & Legal
Education



Logistics

- Format
- How to ask questions
- Webinar will be recorded and available for on-demand viewing

AALS Technology Section Webinar Series

Sydney Beckman

Professor of Law
LMU Law
Knoxville, Tennessee



sydney.beckman@lmunet.edu

Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web
- 4) Digital Marketplace
- 5) Possible Attacks
- 6) Cybercrime as a Business
- 7) How to Protect Yourself

Agenda

- 1) My Background

Professor Beckman

*A somewhat varied
background.*



EQUIFAX®



Southwestern Bell



Agenda

- 1) My Background
- 2) Important Cybercrime Facts

Important Facts

- 1) There is a hacker attack every 39 seconds.
- 2) Hacker attacks affect 1 in 3 Americans every year.
- 3) 43% of cyber attacks target small businesses.
- 4) The average cost of a single data breach in 2020 is expected to exceed \$150 million dollars.
- 5) Over 75% of the health care industry has been infected with malware over the last year.
- 6) 95% of security breaches are due to human error.

Clark School study at the Univ. of Maryland

“Cybercrime is the greatest threat to every company in the world.”

*Ginni Rometty
Chairman, President and CEO
IBM Corporation*

“Cybercrime is the greatest threat to every company, every government, and every individual in the world.”

Professor Beckman



Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web

Three “levels” to the World Wide Web

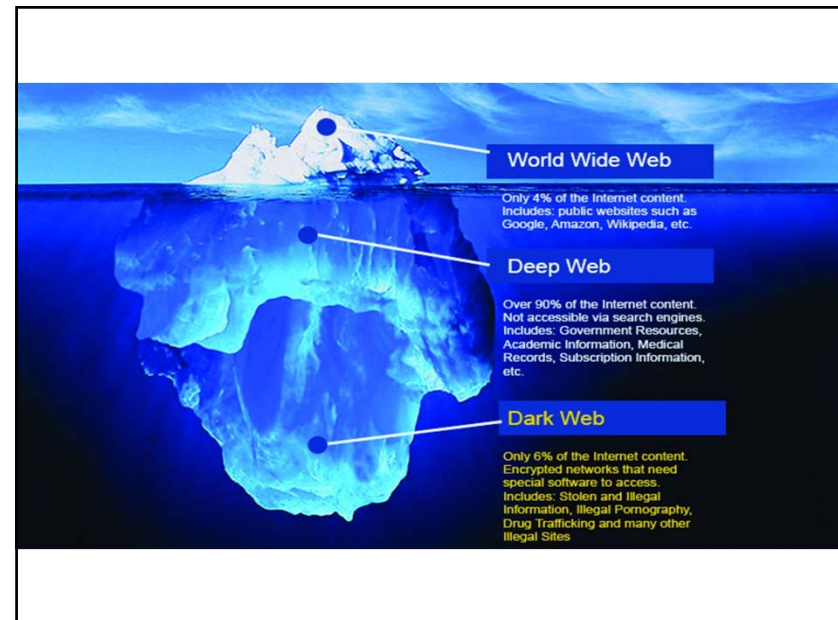
- 1) The surface (or “clear”) web.
- 2) The deep web.
- 3) The dark web.

WARNING

Do not visit the dark web.

Do not conduct ANY transactions over the dark web.

- You risk your career
- You risk your freedom.
- You potentially risk your safety.





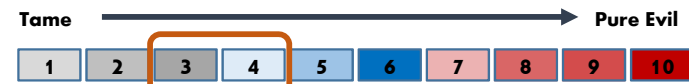
Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web
- 4) Digital Marketplace

The Stuff You Will See Today



The Stuff You Will See Today



Some things you can buy:

Counterfeit USD

Login Register FAQs Products

50 USD BILLS



Our notes are produced of cotton based paper. They pass the pen test without problems. UVI is incorporated, so they pass the UV test as well. They have all necessary security features to be spent at most retailers. Free shipping in the US.

Product	Price	Quantity
25 x 50 USD	400 USD = 0.100 \$	1 x Buy now
100 x 50 USD	1300 USD = 0.324 \$	1 x Buy now

Counterfeit USD

Some things you can buy:

Top-up your pre-paid MasterCard or Visa AND purchase your virtual debit card







Some things you can buy:

Top-up your pre-paid MasterCard or Visa AND purchase your virtual debit card



Some things you can buy:

<p>UK Weed - Skunk - Cannabis - B</p> <p>Clack8102</p>  <p><u>Drugs</u> <u>> Buds</u> BUY from 25\$</p>	<p>★ 4-FA / 4-FMP POWDER </p>  <p><u>Drugs</u> <u>> 4-FA</u> BUY from 226\$</p>	<p>SPAIN DRIVER LICENSE Template</p>  <p><u>Digital Goods</u> <u>> Documents and Data</u></p>	<p>Vicodin</p>  <p><u>Drugs</u> <u>> Opiates</u> BUY from 7\$</p>
--	--	---	---

Some things you can buy:



Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web
- 4) Digital Marketplace
- 5) Possible Attacks

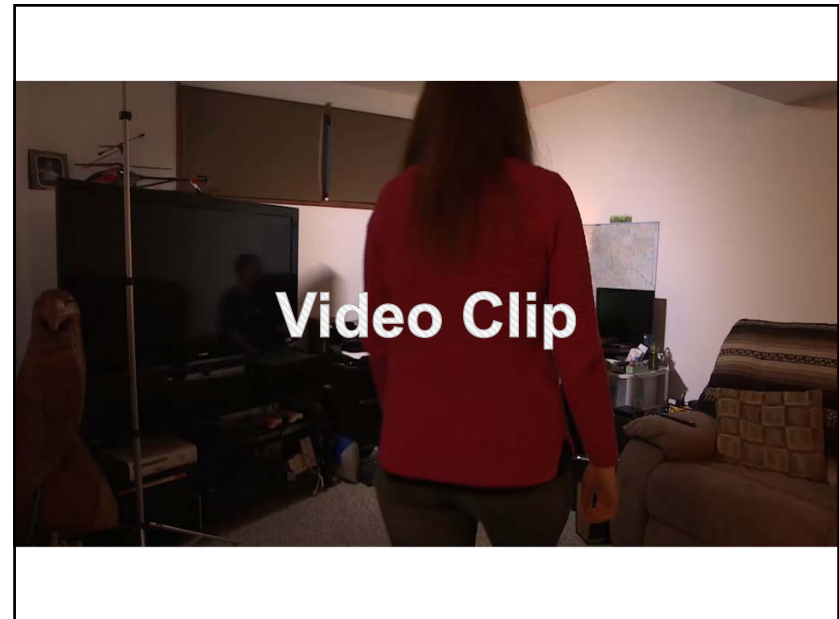
Common Attacks on Individuals & Small Businesses

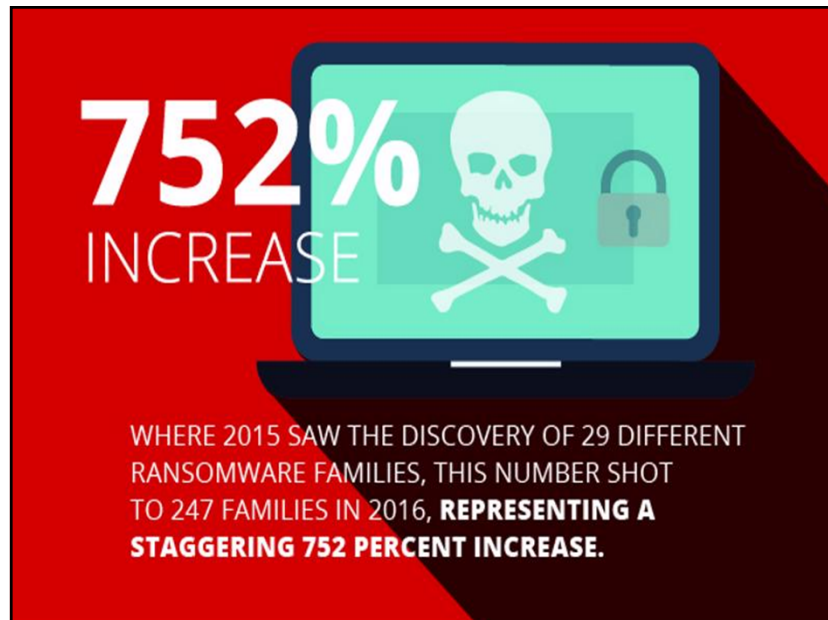
1) **Ransomware**

Ran\$omware

Ransomware is a form of software that prevents users from accessing their systems, files or data until a sum of money is paid.

7/3/2019



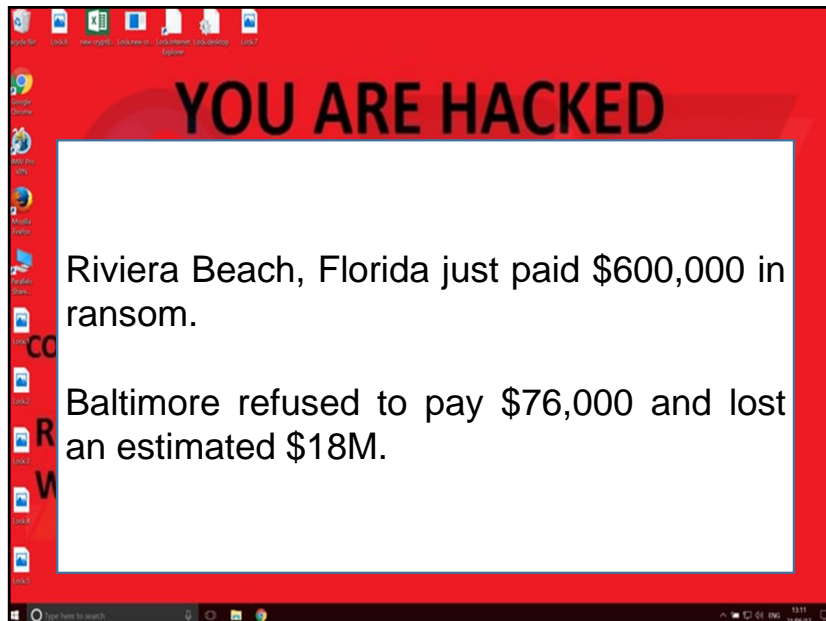


YOU ARE HACKED

A Norwegian aluminum producer is recovering after hackers took 22,000 computers offline at 170 different sites around the world.

The company refused to pay the ransom and have spent \$57M trying to restore their business to full strength.

The screenshot shows a Windows desktop with a red background. At the top, the text 'YOU ARE HACKED' is in large, bold, black letters. Below it, a white box contains two paragraphs of black text. The desktop has a taskbar at the bottom with various icons and a search bar. The system tray shows the date and time as 11:11 7/3/2017.



Common Attacks on Individuals & Small Businesses

- 1) **Ransomware**
- 2) **Identity Theft**

Identity Theft

In 2017, there were 16.7 million victims of identity fraud.



The amount stolen hit \$16.8 billion in 2017. This was an increase over 2016.

For the first time, more Social Security numbers were exposed than credit card numbers.

Common Attacks on Individuals & Small Businesses

- 1) **Ransomware**
- 2) **Identity Theft**
- 3) **Information Theft**

Financial Data

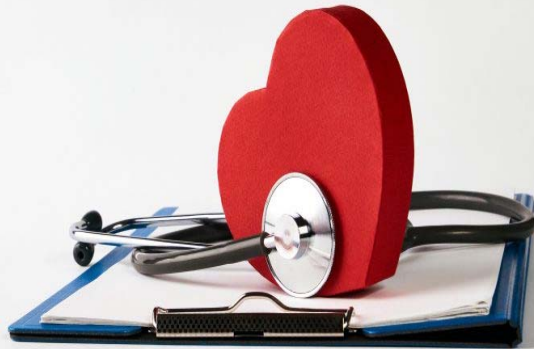
Financial data can be used for:

- ❖ identity fraud
- ❖ loan applications
- ❖ counterfeit credit cards
- ❖ billing accounts or money transfers

With the right details, hackers can even withdraw money directly from victims' bank accounts.

Health Care Details

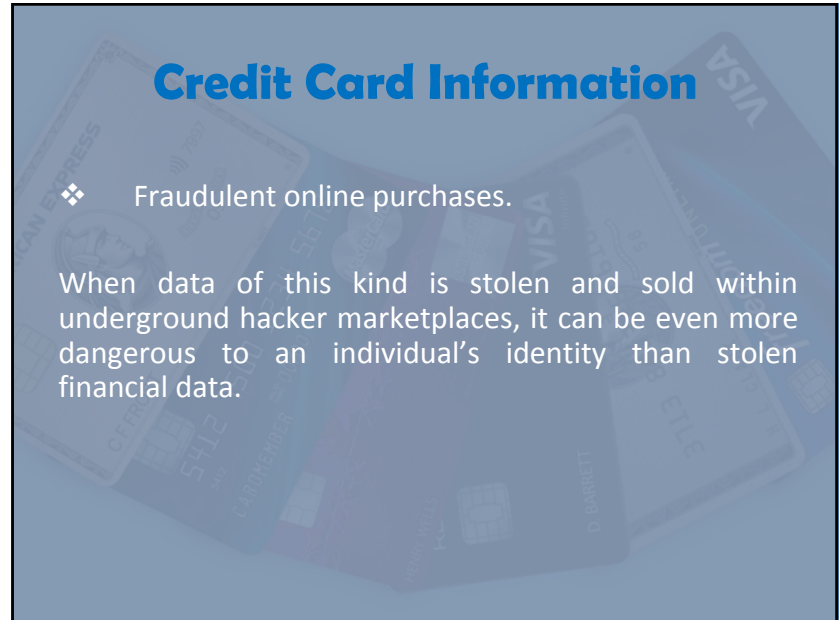
- ❖ Fraudulent insurance claims
- ❖ Fraudulent purchase of prescription drugs.



Credit Card Information

- ❖ Fraudulent online purchases.

When data of this kind is stolen and sold within underground hacker marketplaces, it can be even more dangerous to an individual's identity than stolen financial data.

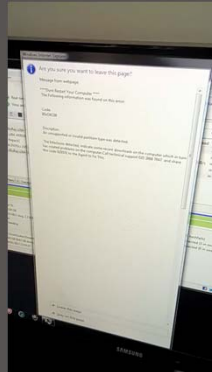


Account Information

Username and passwords can be leveraged by hackers for fraudulent insurance claims, to buy prescriptions, to launch spam or phishing attacks, as well as for extortion or hacktivism, depending upon the account that is hacked.

The Microsoft Scam





Audio Clip

Educational Information

Students transcripts, other school records and enrollment data, can be used for identity fraud and fake student loan applications, as well as for blackmail or extortion.

Common Attacks on Individuals & Small Businesses

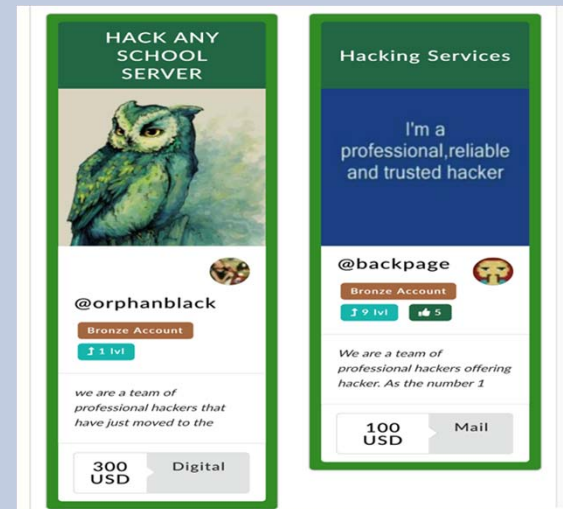
- 1) **Ransomware**
- 2) **Identity Theft**
- 3) **Information Theft**
- 4) **Theft of Passwords**



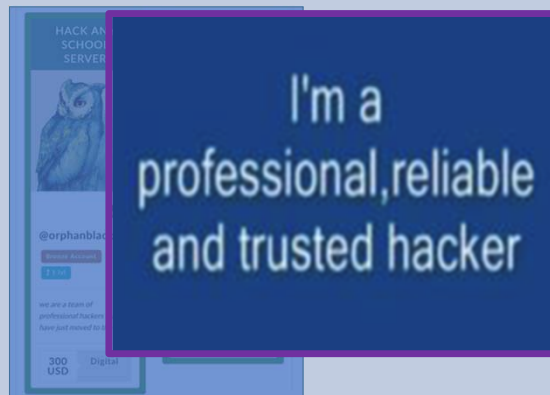
Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web
- 4) Digital Marketplace
- 5) Possible Attacks
- 6) Cybercrime as a Business

Some things you can buy:



Some things you can buy:



Some things you can buy:



Some things you can buy:

6 BITCOIN RANSOMWARE EASY INSTANT DELIVERY

6 BITCOIN RANSOMWARE EASY MONEY 6 BITCOIN RANSOMWARE 0.017 - NEXT 10 ORDER...

Sold by **SPTRLTD** - 18 sold since October 20, 2018 Vendor Level 2 Trust level 1

Unlimited items available for auto-dispatch

	Features		Features
Product Class	Digital	Origin Country	World Wide
Quantity Left	Unlimited	Ships to	World Wide
Ends In	Never	Payment	Escrow

Some things you can buy:

- ▶ I WILL PROVIDE YOU WITH-- 6 ---URLs TO SOURCE CODES, WITH FULL INSTRUCTIONS ON CUSTOMIZING THEM, AND 4 ORIGINAL DISTRIBUTION METHODS.
- ▶ SIMPLY EDIT IT AND SET YOUR OWN PRICE, EMAIL, EXTENSIONS, MESSAGE, TIMER ETC. RANSOMWARE IS EASY TO BUILD AND THERE IS NO REASON WHY YOU SHOULD PAY HUNDREDS FOR ONE THAT YOU CAN EASILY CUSTOMIZE YOURSELF.
- ▶ YOU'LL RECEIVE 4 UNIQUE ★NO EMAIL★ FOOL-PROOF METHODS WITH BETTER THAN 90% PERCENT SUCCESS.

Agenda

- 1) My Background
- 2) Important Cybercrime Facts
- 3) The Deep and Dark Web
- 4) Digital Marketplace
- 5) Possible Attacks
- 6) Cybercrime as a Business
- 7) How to Protect Yourself

Ten + 1 Tips to Protect Yourself

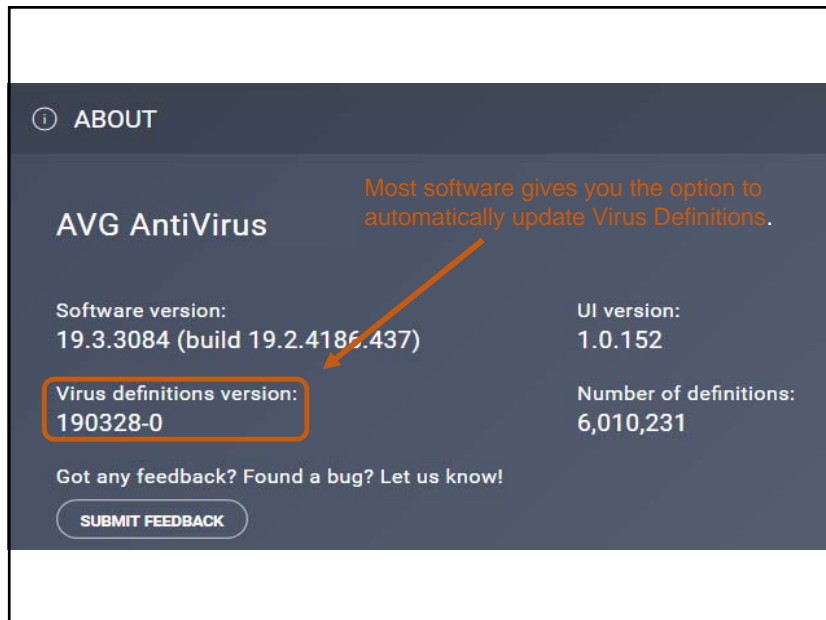
- 1) Backup all important data.

Backup Options



Ten + 1 Tips to Protect Yourself

- 1) Backup all important data.
- 2) Use up-to-date virus protection software.



Always keep your iOS up-to-date



Ten + 1 Tips to Protect Yourself

- 1) Backup all important data.
- 2) Use up-to-date virus protection software.
- 3) Make sure your operating systems are up-to-date.
- 4) Utilize strong passwords that use a combination of letters, capital letters, numbers and symbols.

25 Of The Most Popular Passwords

1	123456	6	123456789	11	admin	16	starwars	21	hello
2	password	7	letmein	12	welcome	17	123123	22	freedom
3	12345678	8	1234567	13	monkey	18	dragon	23	whatever
4	qwerty	9	football	14	login	19	passw0rd	24	qazwsx
5	12345	10	iloveyou	15	abc123	20	master	25	trustno1

Ten Tips to Protect Yourself

- 1) Backup all important data.
- 2) Use up-to-date virus protection software.
- 3) Make sure your operating systems are up-to-date.
- 4) Utilize strong passwords that use a combination of letters, capital letters, numbers and symbols.
- 5) Do NOT share passwords between websites.

In this case – sharing IS NOT caring!!!!



Ten Tips to Protect Yourself

- 6) Use a password wallet or the security measures built into phones.

Ten + 1 Tips to Protect Yourself

- 6) Use a password wallet or the security measures built into phones.
- 7) Be careful with social media information.





The following profile elements can be used to steal or misappropriate your identity:



- Full name (particularly your middle name)
- Date of birth (often required)



- Home town
- Relationship status
- School locations and graduation dates



- Pet names
- Other affiliations, interests and hobbies

Ten + 1 Tips to Protect Yourself

- 6) Use a password wallet or the security measures built into phones.
- 7) Be careful with social media information.
- 8) Use virtual credit cards when buying from small business or foreign websites.

Ten + 1 Tips to Protect Yourself

- 6) Use a password wallet or the security measures built into phones.
- 7) Be careful with social media information.
- 8) Use virtual credit cards when buying from small business or foreign websites.
- 9) Don't send personal information over public Wi-Fi networks.

Example of Passwords Obtained via a Public Wi-Fi Network



The screenshot shows a window titled 'D-Link DWA-121 Wireless N USB Adapter; GUID: {01159A7C-4FDF-4524-980C-A22ECDFE1138}'. The window contains a table with the following columns: SSID, Password, Authentication, Encryption, and Connection type. The table lists three networks: 'Goodbye sega-sega internet', 'Inet from thomson', and 'NEST'. The passwords are obscured by a grey box.

SSID	Password	Authentication	Encryption	Connection type
Goodbye sega-sega internet		WPA-PSK	TKIP	ESS
Inet from thomson		Open	WEP	ESS
NEST		WPA2-PSK	AES	ESS

Ten + 1 Tips to Protect Yourself

- 6) Use a password wallet or the security measures built into phones.
- 7) Be careful with social media information.
- 8) Use virtual credit cards when buying from small business or foreign websites.
- 9) Don't send personal information over public Wi-Fi networks.
- 10) Be aware of your surroundings when typing passwords etc.

Shoulder Surfing



The +1 for the “super careful”

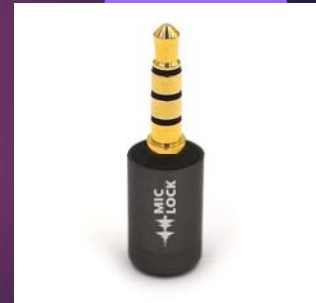
The +1 for the “super careful”

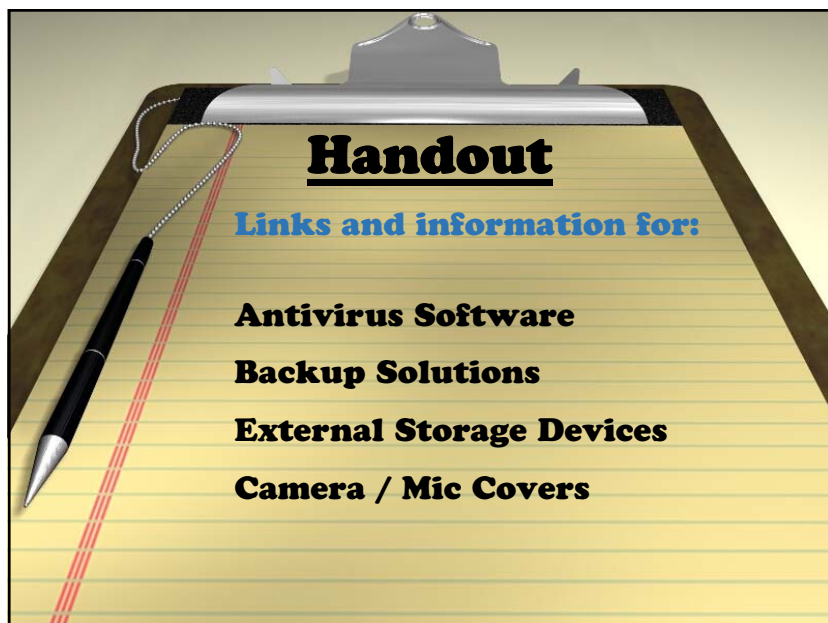
Use a camera cover and microphone lockout.



\$7.99
✓prime

\$6.99
✓prime





Questions & Answers



Sydney Beckman

sydney.beckman@lmunet.edu

Upcoming Webinars

- Tech Productivity Tips for Law Faculty (*July 10*)
- How Law Schools Can Save \$150 Million Using Open Casebooks (*July 17*)
- What Professors Need to Know About Blockchain (*July 24*)

For full list: www.aals.org/sections/list/technology-law-and-legal-education/

AALS Technology Section Webinar Series

Wrap Up

Survey – Your Feedback is Important!

Please consider joining the Section on Technology, Law and Legal Education

Thank you for your attendance!