



# SECURITY IN THE DIGITAL AGE

# OVERVIEW

- Defining the digital age
- Digital security
  - Identity: Personal information
  - Assets: Hardware and data
  - Technology: Software
  - Devices: The Internet of Things (IOT)
- What are the threats
- How to protect yourself
- Resources and recommendations

# DEFINITION OF THE DIGITAL AGE

- Every day, everywhere, digital technology is generating new possibilities; new ways to work and play, to transact and interact. We're surrounded by digital identities and data which need to be exchanged over networks with organizations, people and devices.
- As more and more of these devices get connected, they can help us access a range of services including communications, payment, healthcare and government. The benefits are obvious – but there are security implications too.
- Potentially, there are risks for individual identities as well as personal, corporate and government information.

# DEFINITION OF THE DIGITAL AGE

- To safeguard access to these services, two questions are being asked everywhere, millions of times a second. Not by people, but by devices.
- "Are you who you say you are?" and "Is my data safe with you?"
- Digital Security means answering those questions with solutions that protect and enhance assets and interactions.

# SECURITY THEN AND NOW



- Then

- Security was locking your doors, keeping your mail safe, not giving out your phone number, and shredding important documents
- Attackers were people, were generally local, and had criminal intent

- Now

- Security now also includes keeping all of your digital information and devices secure and monitoring all of the digital information about you that is stored by everybody else
- Attackers are people, governments, software, robots, and other agents, located anywhere in the world, and acting maliciously or frivolously.

# IDENTITY, ASSETS, AND TECHNOLOGY



The classes of digital information are as follows;

- **IDENTITY:** personal information that is stored or shared
  - Government, health care, social media, pictures, maps, financial
- **ASSETS:** hardware and data
  - Your digital devices: how many of you have cell phones?
  - Your digital transactions: how many of you use the internet?
  - Who uses a fitness tracker?
- **TECHNOLOGY:** software
  - The programs (or apps) that you use to process digital information
- **DEVICES:** the internet of things (IOT)
  - What is IOT? “Smart” devices that have only a singular purpose. Examples; NEXT thermostats, smart lightbulbs and light switches, home automation, wireless security systems.
  - In 2016, a major internet hub was brought down by a distributed denial of service (DDoS) attack, possibly through IOT

# IDENTITY SECURITY



- Your **local data** is the information over which you have direct control:
  - Files on your computer
  - A note on passwords and security
- Your **distributed data** is the information over which you do not have direct control:
  - Information stored in the cloud or that you share with others
  - Metadata
  - Location data
  - Social mapping data
  - WiFi history
  - Social networking
  - Website browsing and search history
  - Email
  - Photos
  - Maps
  - Cookies

# PROTECTING YOUR IDENTITY

- Anonymous browsing
  - Use tools and software that do not track your web browsing history
- Add-ons to minimize tracking
  - <https://myshadow.org/prevent-online-tracking>
- Alternative software solutions
  - Mainstream software solutions are preferred targets for identity thieves
  - Free and open-source software (FOSS)
- Know where your data is stored
  - Cloud storage, social media, photos, computer, phone, tablet
  - Software as a solution (SAAS)
- Keeping it fresh
  - Keep your hardware and software up to date
- Read those agreements!



# ASSET SECURITY: DATA

- ASSETS: hardware and data
  - Your digital devices: mobile phones, tablets, computers, laptops
  - Your digital transactions: internet browsing, software as a service (SAAS), cloud storage, apps,
- Loss of data only
  - Leaks: What critical data is lost? What data does it point to? How do you know it has been taken?
  - Damage: What functionality is lost when data is damaged or taken?
  - Theft: Do you know it was taken? What impact will that date have on your life?
- Loss of data through loss of hardware
  - Loss of device / theft of device:
    - What data is stored on a device that is easily stolen or lost?
    - What other data is linked to the lost data?
    - Is all of that data secured?
  - Damage to device:
    - What happens to critical data if a device fails or is missing?

# PROTECTING YOUR DATA



- Assess your risks
  - External risks: who or what might damage your data?
  - Local risks: how might you lose your data?
- Physical: invaders, intruders, and thieves
  - Who is watching over your shoulder?
  - Who has physical access to your devices and data?
  - How can you prevent theft of a portable device?
  - How is your data protected from theft or loss?
- Software risks
  - Keep your software up to date
  - Use a program to help prevent viruses, spyware, malware, etc.
- Encrypt your data
  - Lock your data with encryption, particularly for external data

# PROTECTING YOUR DATA



- Use strong passwords effectively
  - A password should be difficult for a computer program to guess.
    - Make it practical
    - Don't make it personal
    - Keep it secret
  - A password should be difficult for others to figure out.
    - Make it unique
    - Keep it fresh
  - A password should be chosen so as to minimize damage if someone does learn it.

# DATA BREACHES



- Yahoo
- Government human resources office
- Democratic National Committee
- Anthem
- Experian
- You?

# ASSET SECURITY: HARDWARE



## Protect your devices

- Computers
  - Create user accounts
  - Use strong passwords for user login
  - Limit access to computers
- Mobile devices
  - Use strong passwords
  - Encrypt data
  - Install remote locking / wiping on each device
- Wireless networks
  - Use strong passwords on your networks
  - Use caution on unsecured public networks

# PROTECTING YOUR HARDWARE

- Environmental risks: electrical, mechanical, and physical
  - Use surge protectors and battery backups
  - Use a sturdy and clean work environment
  - Avoid possible accidents
    - No coffee on your desk
    - Hide those cables
- Back up regularly
  - Hard drives don't last forever

# TECHNOLOGY SECURITY: SOFTWARE

- TECHNOLOGY: software
  - The programs (or apps) that you use to process digital information
- Purchased software
  - Know who wrote and owns the software. Make sure you buy licensed versions, not knock-offs.
- Web applications
  - Do you really need to do this?
  - Know where you are going and what you are clicking
- Software as a service (SAAS)
  - Know who owns the software, their privacy policies, and their data sharing practices. Read the agreements.

# PROTECTING YOUR SOFTWARE



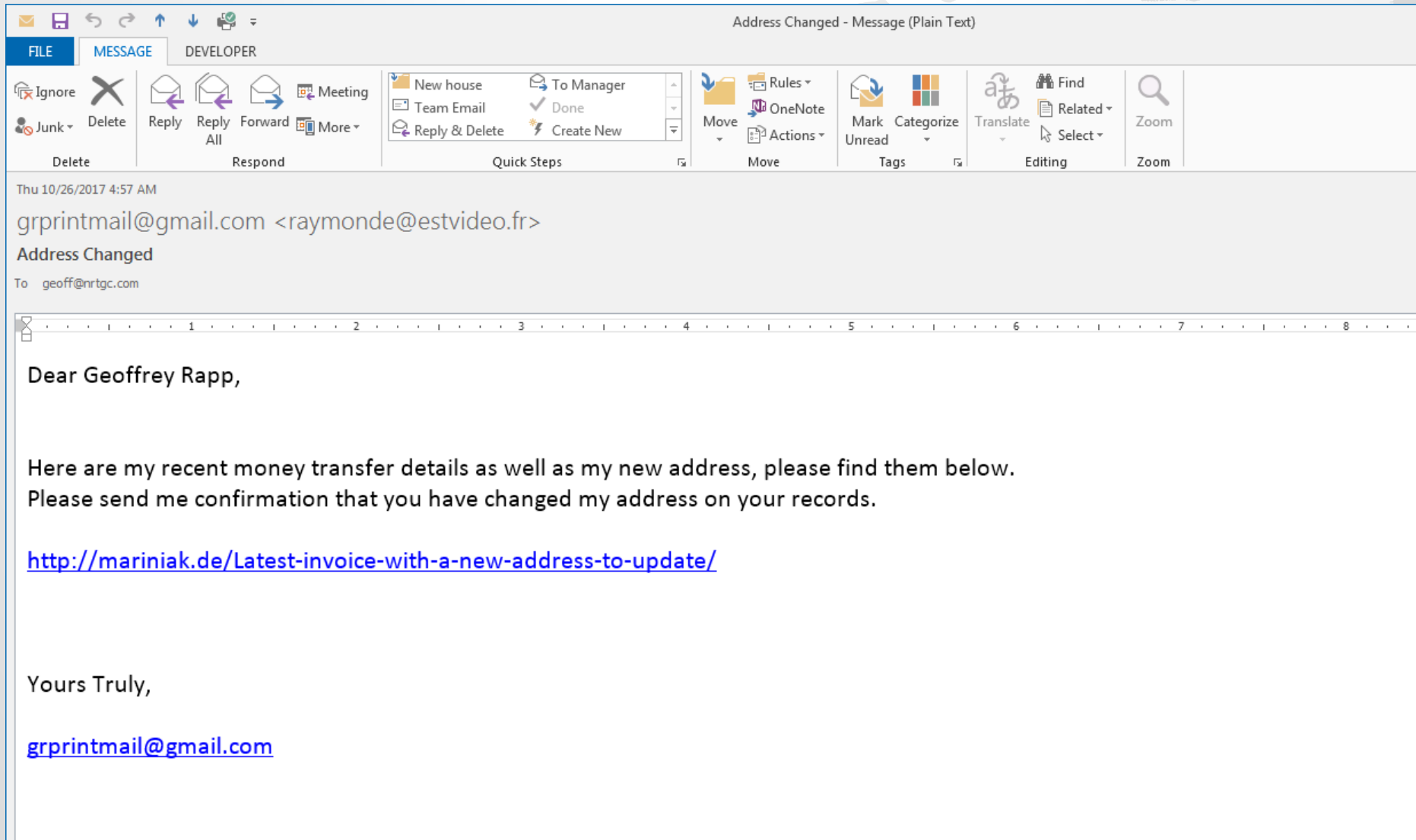
- Keep it up to date
  - Make sure to check and install security updates
- Be aware of who wrote the software
  - Only use licensed versions of software
- Be aware of the security of web-based software
  - Know who owns and operates the software
- Look for the lock
  - HTTP vs. HTTPS



# DEVICE SECURITY: INTERNET OF THINGS

- DEVICES: the internet of things (IOT)
  - What is IOT? “Smart” devices that have only a singular purpose. Examples:
    - NEST thermostats, smart lightbulbs and light switches, home automation, wireless security systems, smart electric meters.
    - In 2016, a major internet hub was brought down by a distributed denial of service (DDoS) attack, possibly through IOT
    - Ad-hoc networking
- Wireless security systems
  - They are being promoted because of “wire-cutting”
  - They generally do not have robust security protocols
- Limit your use of these devices, or be very aware of the risks
- Make sure to use strong passwords wherever possible

# A WARNING ABOUT EMAIL



The screenshot shows an Outlook email window. The title bar reads "Address Changed - Message (Plain Text)". The ribbon is set to "MESSAGE". The email content is as follows:

Thu 10/26/2017 4:57 AM  
grprintmail@gmail.com <raymonde@estvideo.fr>  
**Address Changed**  
To: geoff@nrtgc.com

Dear Geoffrey Rapp,

Here are my recent money transfer details as well as my new address, please find them below.  
Please send me confirmation that you have changed my address on your records.

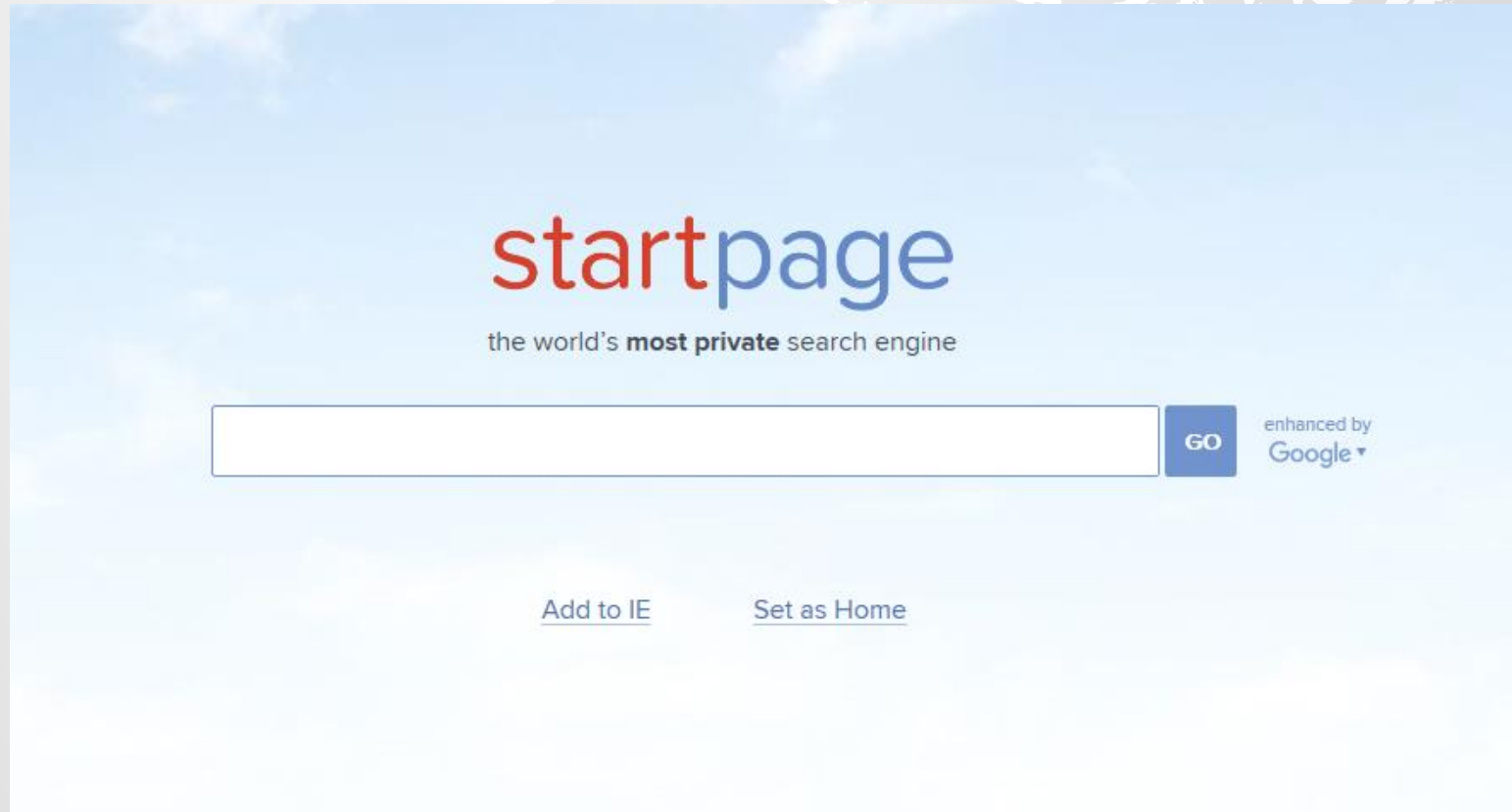
<http://mariniak.de/Latest-invoice-with-a-new-address-to-update/>

Yours Truly,  
[grprintmail@gmail.com](mailto:grprintmail@gmail.com)

# A WORD ABOUT WEBSITES

The screenshot shows a web browser window with the URL <http://ccm.net/download/>. The browser's address bar and tabs are visible at the top. The main content area has a navigation menu with categories like 'Ask a question', 'Windows Software', 'Mac Software', 'Linux Software', 'Android Apps', 'BlackBerry Apps', 'iPhone Apps', and 'Windows Phone Apps'. Below the menu is a large banner for 'on us' with a '\$100' logo and an 'Upwork' logo with a 'Limited time!' tag. The main content area is titled 'Download' and features a search bar with 'All categories' and a search button. Below the search bar, it shows 'Results 1 - 30 of about 9,000'. There are two sponsored links: 'CCM - Live forum for iPhone & iPad' and 'Google Play Store'. The 'CCM' link includes a red question mark icon, a 5-star rating, and a 'Download' button. The 'Google Play Store' link includes a Google Play icon, a 5-star rating, and a 'Download' button. On the right side, there is a large green 'START DOWNLOAD' button, a section for 'Free DIY & How-To Videos' with a search icon, and a 'You May Like' section with a photo of two men and a link to 'Bay Village, Ohio: This Brilliant Company Is Disrupting a \$200 Billion Industry'.

# A WORD ABOUT WEB SEARCHING



# WHAT TO DO

- Awareness: be aware of potential digital risks, write them down, assess the impact of each, and what can be done about it.
- Technology: increase your technological competency and available solutions
- Use anti-malware software
- Strengthen your passwords
- Encrypt your data
- Be aware of attempts to access your data, particularly email
- Be careful when sharing information with others
- Be aware of where your information is stored
- Practice Safe Social Media

# TOOLS

- Passwords and access control
  - <https://www.keepassx.org/>
- Encryption
  - <https://www.upwork.com/hiring/development/introduction-to-encryption-data-security/>
- More secure browsing
  - <https://www.torproject.org/>
  - <https://www.mozilla.org/en-US/firefox/new/>
- Anti-malware
  - <https://www.avast.com/en-us/index>
  - <https://www.pandasecurity.com/usa/>

# TOOLS

- Anti-theft devices
  - <https://www.kensington.com/us/us/home>
- Tracing analysis
  - <https://myshadow.org/trace-my-shadow>
- Free and open-source software (FOSS)
  - <https://www.gnu.org/>

# RESOURCES AND REFERENCES

- Remember, even using these links may subject you to data-tracking
- Your digital shadow: <https://myshadow.org/>
- Security in a box: <https://securityinabox.org/en/>
- Seven steps to digital security: <https://ssd.eff.org>
- Generation safe: <http://generationsafe.ikeepsafe.org/>
- 11 amazing facts: <http://www.gb-advisors.com/>
- A glimpse at tracing and tracking: <https://www.acxiom.com/>