Security Awareness Brief

By Daniel Kawuma <dkawuma@renu.ac.ug>

Security Awareness

School's Network Design

cert@renu.ac.ug

15th – 18th May, 2023

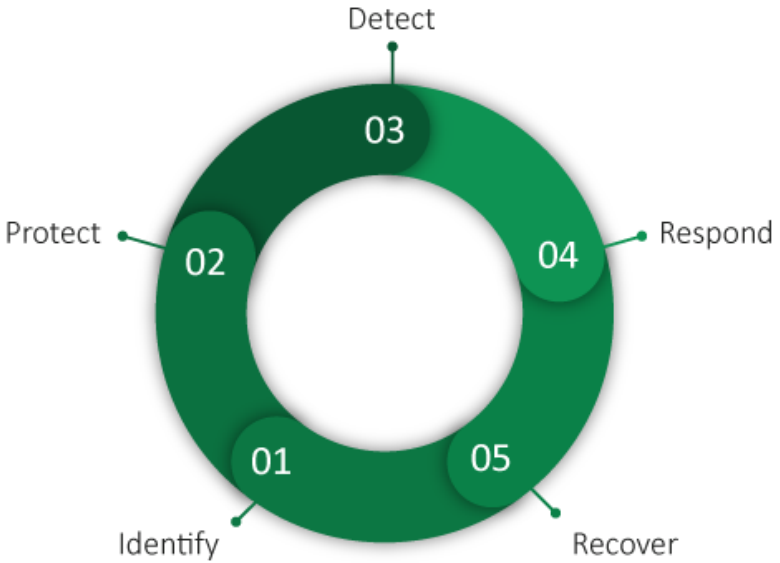
Outline

- Security Process
- Policy Framework
- Cyber Threats
- Countermeasures
- Web Security
- QnA + Discussion


Security is a process,
not a product.
Bruce Schneier
quotefancy

The Security Process…

- Prepare for future problems
  - Hackers, Viruses, Ransomware
- What is at risk
  - Student data, finances, Email systems, IoTs
- Efforts to mitigate the risk
  - Strong passwords, 2FA, Biometric Authn
- Monitor for breaches and IoCs
  - Windows Defender, Windows Firewall
- Have a response plan
  - Containment, Backups, User training
- Restore operations after an incident



Policy Framework

- Why Policy is important?
  - Permissible, Disallowed activities
  - Specify how you want people to behave
- Enforcement of the policy
  - Firewalls, Application filtering
  - Link to your disciplinary procedure
  - Monitor network activity
  - Consequences
- Google “School AUP” for templates

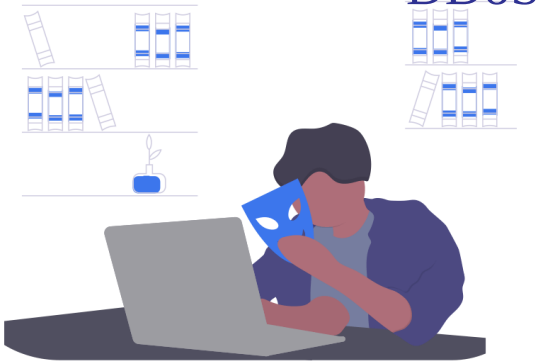
Cyber Threats

Phishing

Ransomware

DDoS

Malware

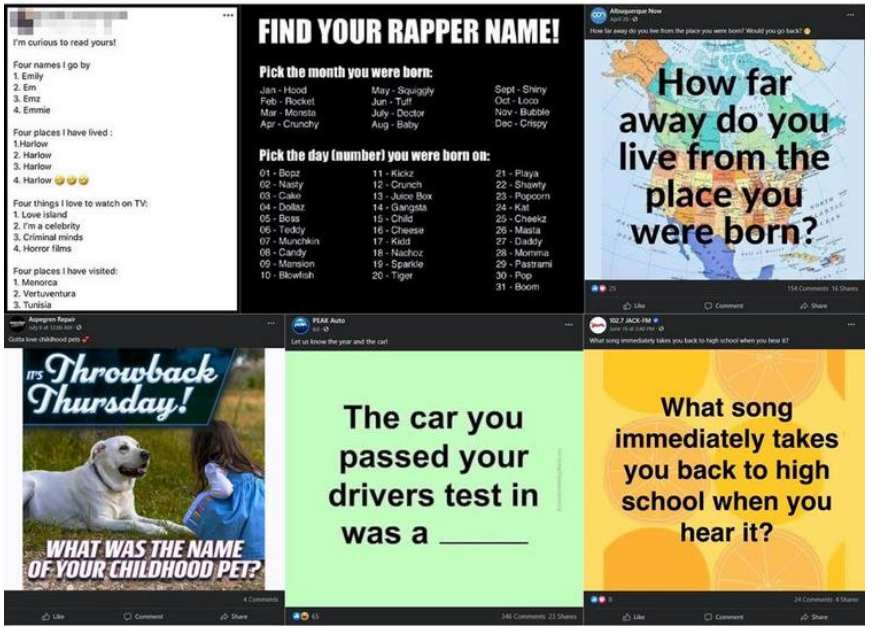


Insider Threat

Cyber Threats: How we are hacked…

How people think they get hacked:

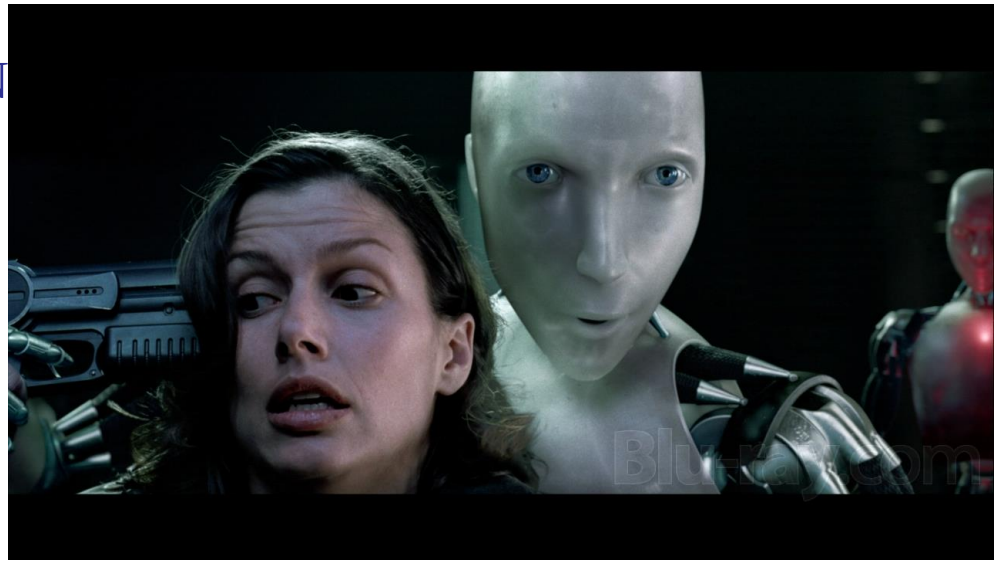
How they really get hacked:




THINK YOU are TOO SMALL
TO GET HACKED?
Think Again

Behavior of a Compromised Machine…

- Outbound connections to CnCs
- Attack other machines on the LAN
- Start spewing Spam
- Anti-virus alerts
- Slow speeds
- Pop-ups or Ads



Virus Protection

- Spread through user actions
  - Poor browsing habits
  - Opening email attachments
  - Clicking “OK” or “Install” when you shouldn’t
  - Clicking malicious links
- A firewall is not “enough”

- Keep all systems updated
- Free windows protection
  - Windows 10: Windows Defender
  - Windows 8.1: Windows Defender
  - Windows 8: Update to Windows 8.1
  - Windows 7: Disabled security essentials and install virus protection
  - Windows XP: Throw them out

Users’ machines don’t get infections without the user’s help

Countermeasures…

- Get rid of obsolete operating systems
- Use built-in security features
  - Don’t turn off built-in firewalls
- Network-based containment
- User education
  - Human firewalls
  - No quick fix
- Keep all systems updated
- Traffic Filtering
  - Outbound ports to block:
    - 25/TCP – Unauthenticated SMTP
    - 123/UDP - NTP
    - 135-139/TCP & UDP – NetBIOS
    - 389/UDP - cLDAP

Web Security

Outline

- Privacy
- Web Safety
- QnA + Discussion

Privacy on the Internet

Unpacking the Privacy Paradox

The privacy paradox is a dichotomy between **a person's intentions to protect their online privacy versus how they actually behave online** and, as a result, compromise their privacy.

Burglars jailed for holiday raid on John Terry's mansion

The gang targeted John Terry's home after spotting images posted online by him during his skiing holiday in the Alps

Mirror FOOTBALL CELEBS TV ROYALS MONEY

Jennifer Lawrence leaked nude photos: Apple iCloud password hack could be 'responsible for security breach'

Tech experts are now saying weak passwords gave hackers the chance to access private pictures thanks to a software glitch

By David Raven
13:41, 1 Sep 2014 | UPDATED 10:37, 23 Sep 2014

BOOKMARK

Kirsten Dunst tweeted her response to the leak, expressing her anger through the medium of emoji.

Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince'

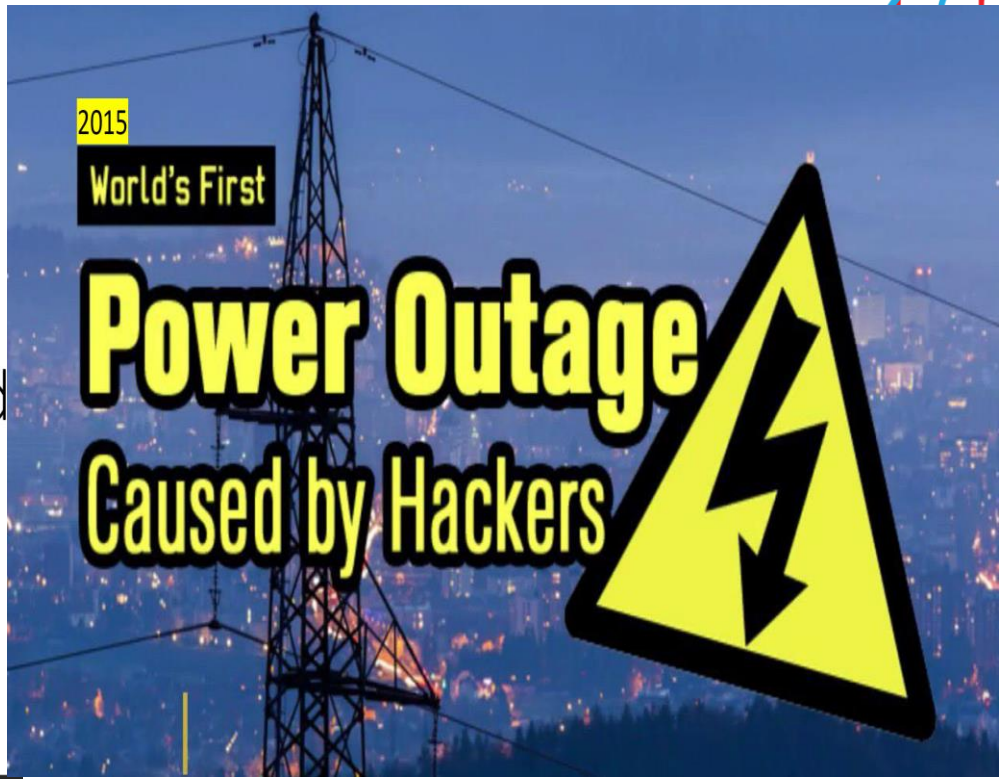
Exclusive: investigation suggests Washington Post owner was targeted five months before murder of Jamal Khashoggi

Revealed: the Saudi heir and the alleged plot to undermine Jeff Bezos

Jeff Bezos, the Saudi crown prince, and the alleged phone-hacking plot – video explainer

The Amazon billionaire Jeff Bezos had his mobile phone "hacked" in 2018 after receiving a WhatsApp message that had apparently been sent from the personal account of the crown prince of Saudi Arabia, sources have told the Guardian.

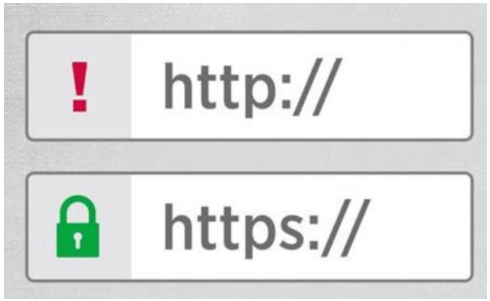
2014: Sony Pictures hacked by North Korea



2015: Madison Ashley data leak

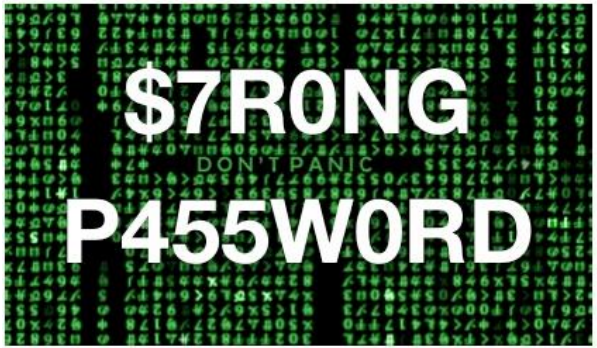
- 25gb of company data stolen (emails, user data)
- Usernames & paswords from customers put online
  - Suicide, divorce and public humiliation

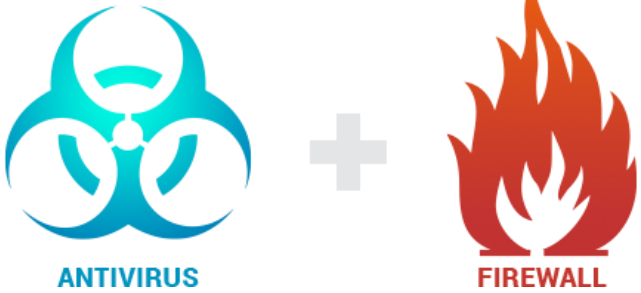
Web Safety


http://
https://


Password Manager

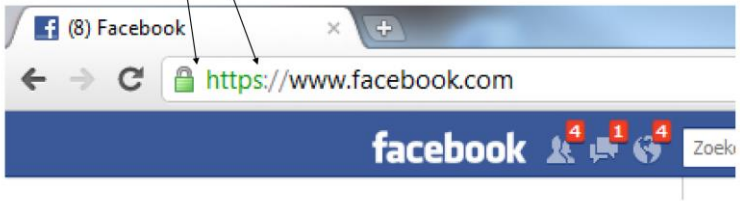

VPN


$7R0NG
DON'T PANIC
P455W0RD


ANTIVIRUS
FIREWALL


MFA
Password
Verification
Access

Use **https** if possible…always.



Log out…always

- Otherwise others might be able to take over your session
  - Be certain to log out on devices that are not yours (e.g. school pc)
  - Log out when using public networks

Follow these web safety rules!!!

DO

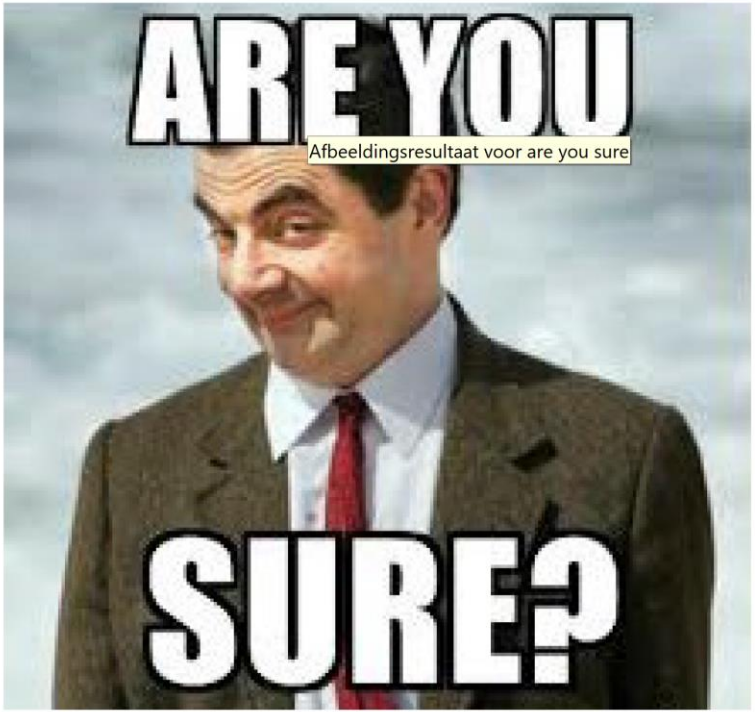
- Use **HTTPS** sites
- Use a **trusted VPN**
- Use password managers
- Use **STRONG** passwords
- Setup **MFA** if possible
- Update your browser & extensions **regularly** to **stable** versions
- Use **different** browsers
- Update & enable **trusted** FW + AV

DON'T

- Save passwords in browsers
- Click links carelessly
- Share **too much** information online
- Download and install **untrusted** apps
- Ignore software updates
- *Share any passwords

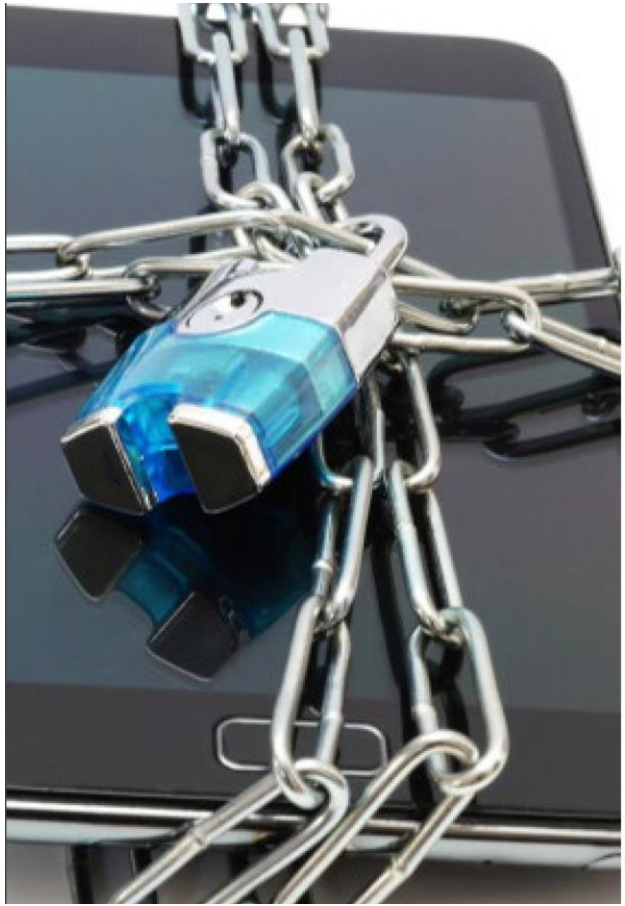

DATA
WITH GREAT POWER COMES GREAT RESPONSIBILITY..

My phone can’t be hacked!



Famous last words

The unhackable ‘smart’phone



Don’t forget your weakest hardware link

- Secure your mobile phone/tablet (minimum Pincode)
- You always carry a gigantic data-source with you
- Can easily e stolen

- Never use unofficial apps!
- Only install ‘store’ apps (but remain vigilant)


It's like the Wild West, the Internet. There are no rules.
Steven Wright
quotefancy

QnA + Discussion

Write to cert@renu.ac.ug
For anything cybersecurity-related

SECURITY IS **EVERYONE'S** RESPONSIBILITY