Cyber Security 101 for End Users

NETWATCHER™

By Defensative

Info@Defensative.com

✓Social engineering – You are your companies biggest security risk!

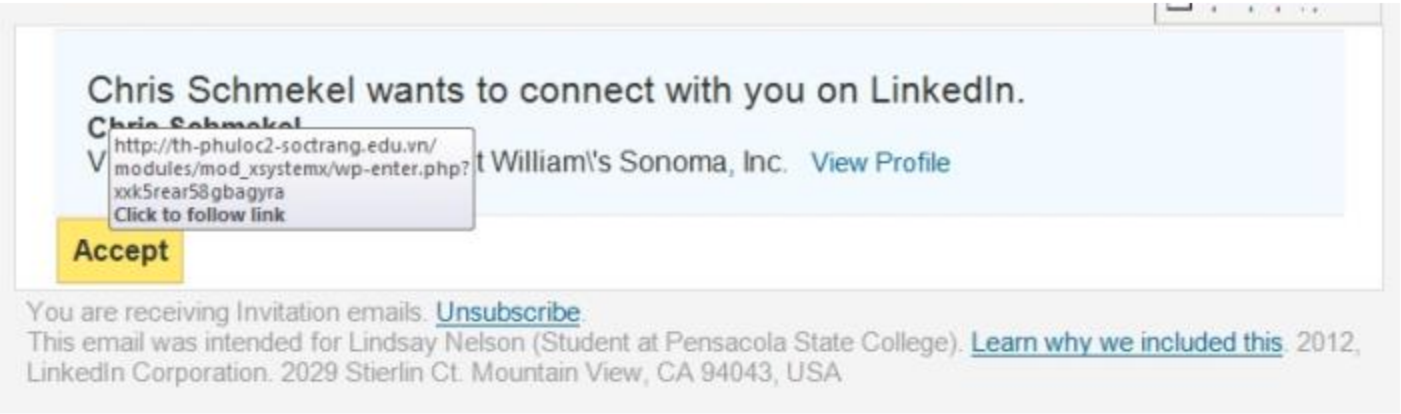
You may receive a fake email or text message with a website created to look like it’s from an authentic company.

What it does:

- Trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner than seems official and intimidating, to encourage you to take action.
- Convince you to download Malware

39 Percent of Employees Admit to Opening Suspicious Emails

Example:



Chris Schmekel wants to connect with you on LinkedIn.

Chris Schmekel

V… t William\'s Sonoma, Inc. View Profile

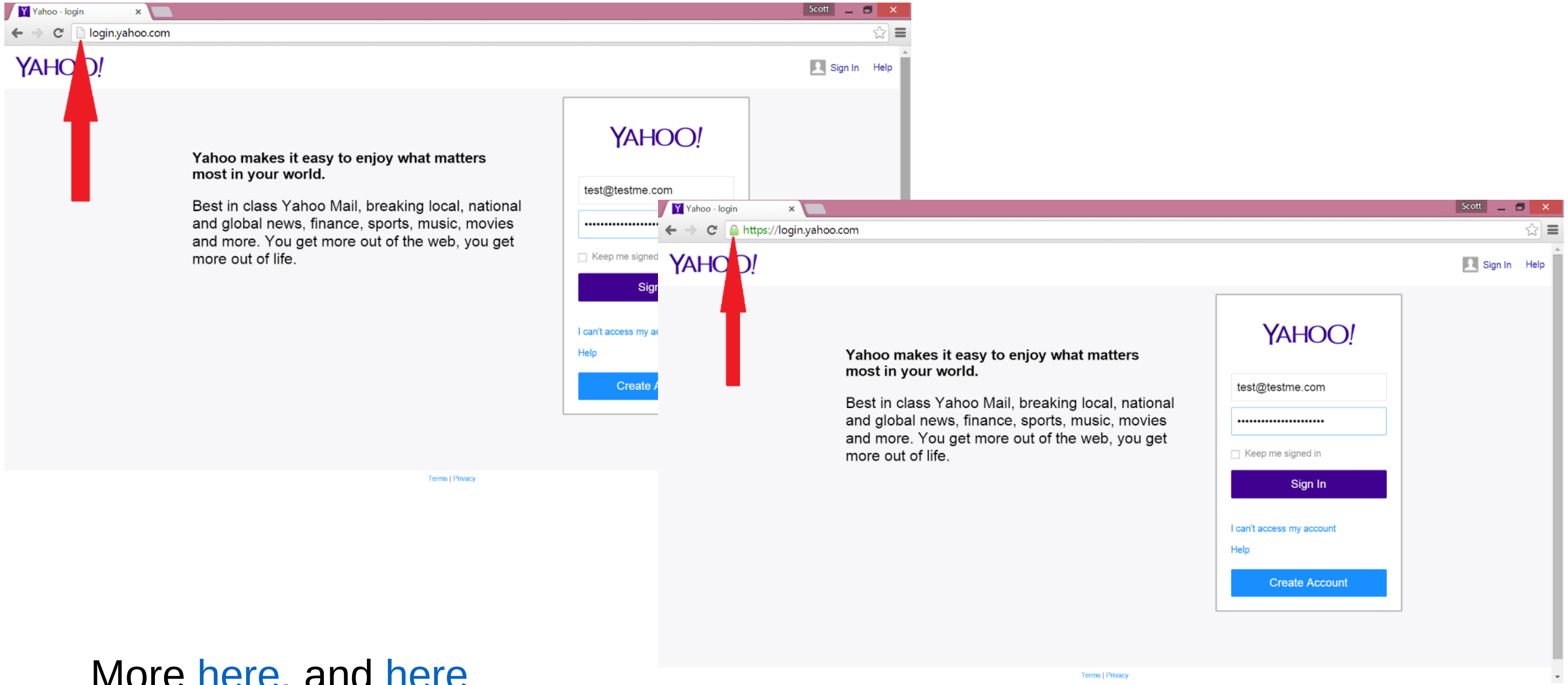
http://th-phuloc2-soctrang.edu.vn/modules/mod_xsystemx/wp-enter.php?xxk5rear58gbagyra
Click to follow link

Accept

You are receiving Invitation emails. Unsubscribe.
This email was intended for Lindsay Nelson (Student at Pensacola State College). Learn why we included this. 2012, LinkedIn Corporation. 2029 Stierlin Ct. Mountain View, CA 94043, USA

✓Use HTTPS (note the “S”)

Unfortunately many websites and services today still offer un-encrypted login. With un-encrypted login, the password is NOT encrypted and considered "cleartext" and can be easily decoded!



Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

test@testme.com

Yahoo makes it easy to enjoy what matters most in your world.

Best in class Yahoo Mail, breaking local, national and global news, finance, sports, music, movies and more. You get more out of the web, you get more out of life.

test@testme.com

More here, and here

✓Keep software up to date

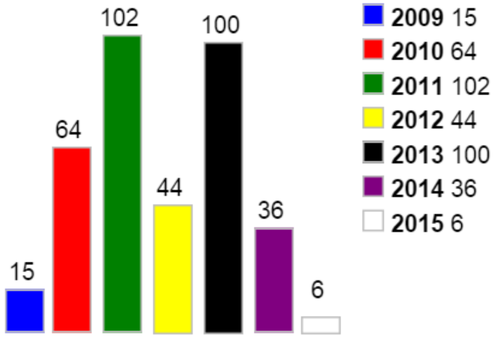
Software vendors such as Adobe, Microsoft, Oracle and others produce frequent security patches that plug holes that can be exploited by bad actors.

If you don't install these patches on a regular basis on your hosts, desktops, laptops and phones your infrastructure will be at risk and will eventually be compromised.

CVE Details is a good place to keep up on the patches. They consolidate vulnerability data from the National Vulnerability Database (NVD) and www.exploit-db.com . Another great site is Mitre's CVE site here .

Here are 2 examples to give you some perspective on how many vulnerabilities a software can contain:

- Here is a list of Adobe Flash vulnerabilities.
- Here is a list of Oracle Java vulnerabilities.
- Here is a simple chart that shows how many vulnerabilities have been published over the years in the Windows 7 OS



✓Don’t use risky software

Examples:

- BitTorrent - you have no control over what the BitTorrent user is downloading and you don't want to end up like this guy . (or these people)
- TOR – You don’t know who is sniffing on the exit nodes (example)
- TFTP – It’s all in clear text (more)
- Misc Android Apps – 97% of mobile malware is on Android (more) (example)

✓Passwords

- Use Secure Passwords (more)
- Use throw away passwords on non-mission critical sites
- Understand Password Managers may not be that secure (example)
- Change Default Passwords! (more)
- If available enable two factor authentication (example)

✓Your Phone

Tips to Prevent Mobile Malware

- Understand the mobile risks - A mobile device is a computer and should be protected like one. If you access the corporate network with their mobile device you should understand the risk imposed by downloading applications and accessing website that are not from trusted sources. You need to also know the value of keeping your operating system on the device up to date with the latest security patches from the manufacturer/mobile provider and operating system vendor.
- Only access corporate data via Wi-Fi over a secure tunnel as over the air networks are exposed to malicious capturing of wireless traffic. There are several mobile Virtual Private Networking technologies (VPN) that can be deployed that can allow users to connect through these secure tunnels.
- Understand your group's Bring Your Own Device to work (BYOD) policies
- Ask your organization if they have a Mobile Device Management (MDM) platform and Mobile Application Management Platforms from companies like Good and others.
- Encrypt your devices - It is very difficult for someone to break in a steal data on an encrypted device (this goes for the SIM card as well).
- If you use Android then use anti-malware software

✓Home network and public WIFI’s

- Change the default password and keep the firmware up to date on your home internet router
- Don’t connect to random WIFI’s (example)
- Don’t allow others to download programs to computers or phones that will connect to your companies network.   Here is a Minecraft example.
- Use a Virtual Private Network (VPN) (example, example)

✓Explicit sites

Pornography and Malware… They go together. (more)

Visitors to Pornhub.com, the 63rd most popular website in the world (and 41st in the US) have a 53% chance of coming into contact with malware

✓Know what to do… https://www.fbi.gov/report-threats-and-crime

Great advice from SecurityMetrics (here)

- **Disconnect** from the Internet by pulling the network cable from the router to stop the bleeding of data. Do not turn off your computer/phone/tablet
- **Follow** your groups cyber security policy step by step plan. Your group will usually:
  - **Document** all network changes, notification/detection dates, and people/agencies involved in the breach
  - **Segregate** all hardware devices in the payment process, or devices suspected of being compromised (if possible) from other business critical devices.
  - **Quarantine** instead of deleting.
  - **Preserve** firewall settings and firewall logs
  - **Restrict** Internet traffic to only business critical servers and ports outside of the credit card processing environment.
  - **Disable** (do not delete) remote access capability and wireless access points.
  - **Call a PFI.** Once the breach is contained by steps 1-7, consult with a forensic PFI to plan a compromise analysis.