Cyber Security Checklist

Threats & Countermeasures

www.mysecurityconsole.com
info@mysecurityconsole.com

Cybersecurity Checklist

Use this guide to identify what you can do to protect your organization from cyber threats. This is not an exhaustive list; it is strongly recommended that you seek professional assistance to select and implement security measures that are appropriate for your organization's applications and data.

IDENTIFY

- □ A list of all assets and data that need to be protected is created and maintained
- □ Risks to data and assets are identified and prioritized
- □ Legal and regulatory requirements are understood and managed

PROTECT

- □ At least two data backups exist using separate media with off-site copies
- □ Backups that contain confidential, private or sensitive data are encrypted
- □ Backups are periodically tested and verified
- □ Whole-disk encryption is used for laptops, smartphones and USB drives
- □ Email security includes malware scanning, phishing protection, and spam filtering
- □ Anti-virus is used for all systems including servers, PCs and smartphones
- □ Safe browsing technology such as anti-virus plugins and ad-blocking is used
- □ Strong passwords are enforced through training, policies and technology
- □ Internet / cloud based user accounts are protected with two-factor authentication
- □ Software updates and patches are tracked and applied to all IT systems and devices
- □ All users receive training including awareness, policies and best practices
- □ Intrusion Prevention Systems are used and actively monitored

DETECT

- □ The network is monitored to detect potential cybersecurity events
- □ Events are monitored and analyzed, incident alerting capabilities exist
- □ Websites and other internet services are scanned for malicious code
- □ Threat and vulnerability information is monitored for key applications
- □ The local network and cloud services are scanned to verify access restrictions

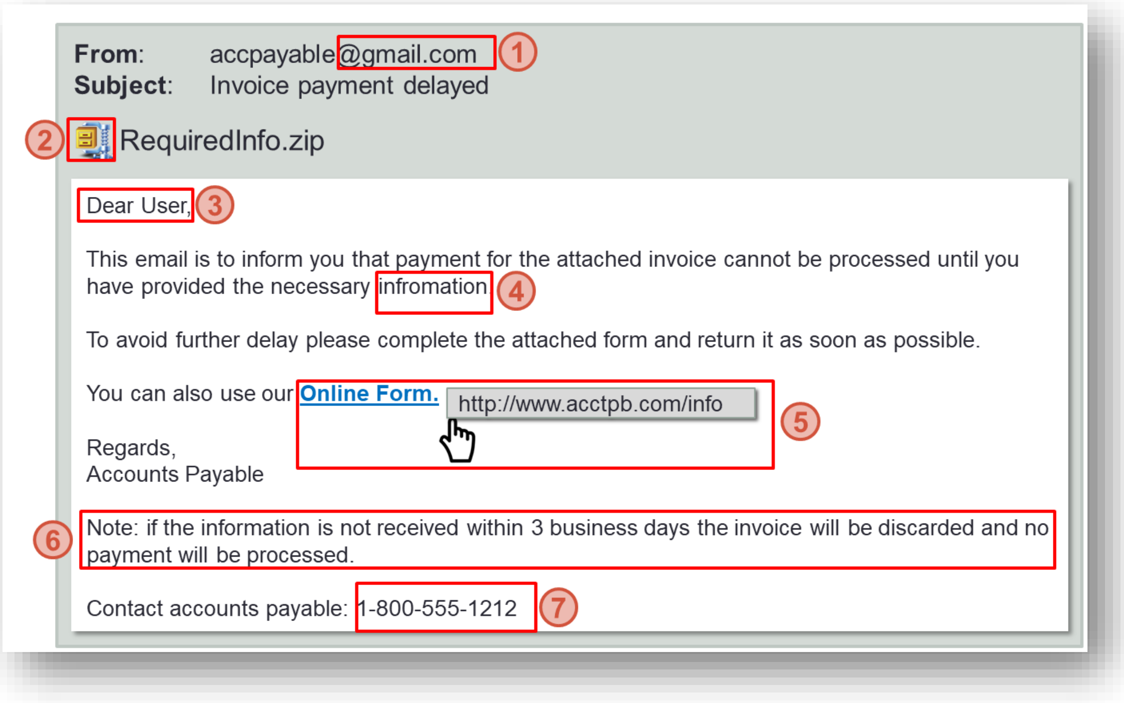
RESPOND

- □ A cyber incident response plan is in place and managed
- □ Personnel have been trained on incident response roles and responsibilities
- □ Events and notifications from detection systems are investigated
- □ Events are reported in accordance with regulations and established criteria

RECOVER

- □ Incident response plan includes lessons learned and plan updates
- □ The root cause of each incident is understood and mitigated

Phishing



From: accpayable@gmail.com
Subject: Invoice payment delayed

RequiredInfo.zip

Dear User,

This email is to inform you that payment for the attached invoice cannot be processed until you have provided the necessary infromation

To avoid further delay please complete the attached form and return it as soon as possible.

You can also use our **Online Form.** http://www.acctpb.com/info

Regards,
Accounts Payable

Note: if the information is not received within 3 business days the invoice will be discarded and no payment will be processed.

Contact accounts payable: 1-800-555-1212

What to do

□ Train yourself to look for clues in every email

1. Make sure the sender email address is valid, pay attention to the domain
2. Don’t trust unsolicited file attachments
3. Be suspicious of generic greetings
4. Be aware of spelling or grammatical errors
5. Don’t trust links, use the hover feature to see where they link to
6. Keep an eye out for threats or urgency
7. Don’t trust phone numbers in email, look them up on the web

□ Never give out sensitive information in response to an email

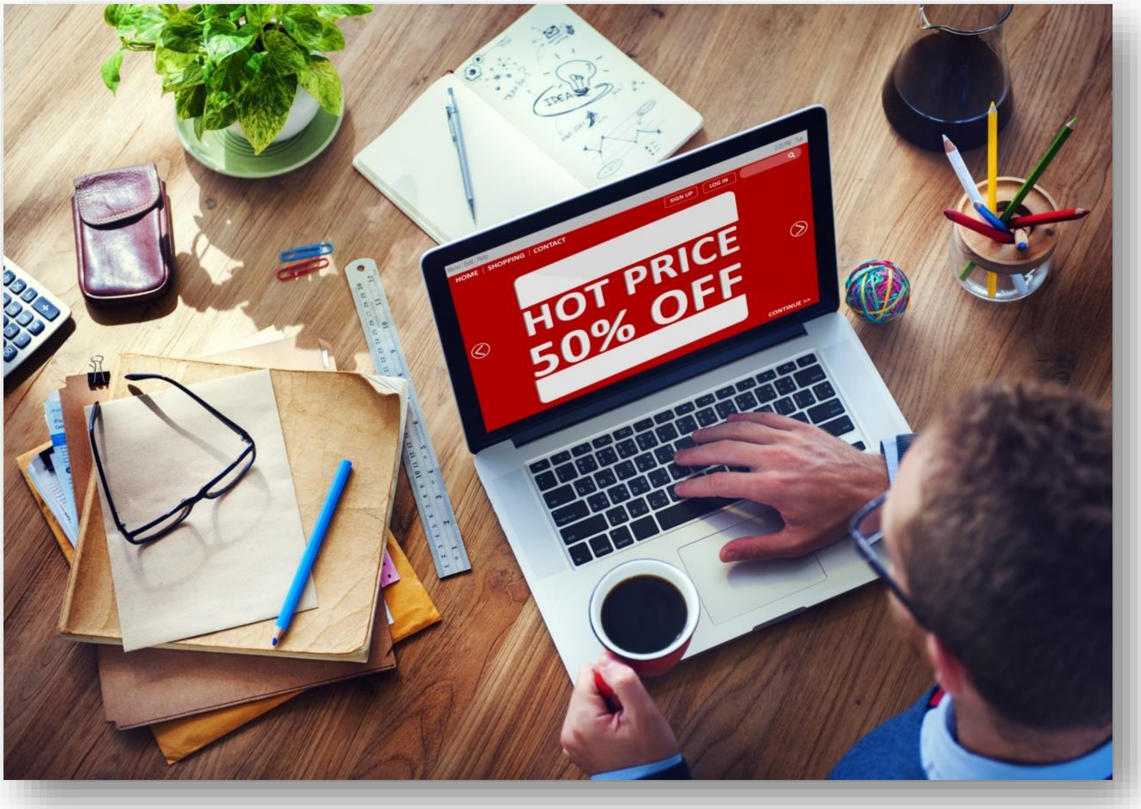
□ If there are any clues use other means to verify the message authenticity

□ When you do open attachments in legitimate email, don’t enable macros

□ Remember spear-phishing and whaling may use authentic looking email

□ Set a recurring reminder to learn about the latest phishing trends every month

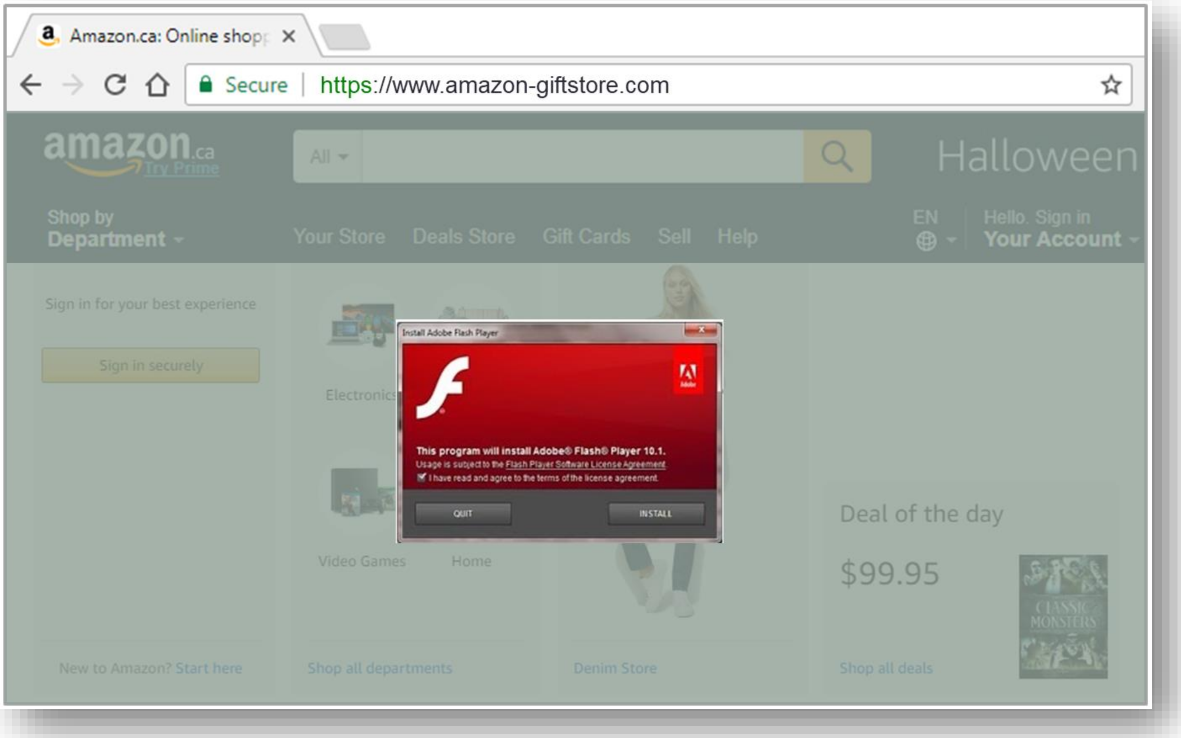
Malvertising



What to do

- □ Avoid clicking on internet ads when possible no matter what site you're on
- □ Keep your computer software up to date, especially the OS, browser, browser plugins, Java, flash player and PDF reader.
- □ Use anti-virus software
- □ Enable browser add-ons that are included in your anti-virus
- □ Use an ad blocker
- □ Learn exactly what your browser's security indicators and features mean

Exploit Kits



This program will install Adobe® Flash® Player 10.1.
Usage is subject to the Flash Player Software License Agreement.
☑ I have read and agree to the terms of the license agreement.

What to do

- □ Make sure you're not spreading malware from your website
    1. Protect administrative logins with two factor authentication
    2. Keep your website software up to date
    3. Keep track of vulnerabilities with web server components
    4. Use external scanners
    5. If you use a web hosting company ask how they do these things
- □ Keep your computer software up to date, especially the OS, browser, browser plugins, Java, flash player and PDF reader.
- □ Use anti-virus software
- □ Enable browser add-ons that are included in your anti-virus
- □ Avoid using browser plug-ins, look for and disable any that you have but don't need