



# United Technologies

## IT Security Awareness Website

Every year, UTC IT Security participates in Cyber Security Awareness Month. We revamp our Security Awareness website with new games, resources, videos and links each year. With weekly October updates, users come back to increase not only their basic knowledge on things like email spam and phishing, but also their knowledge on IT Policies, encryption, and different tools UTC has to help keep the network safe.

# Homepage

The screenshot shows the homepage of the United Technologies Security Awareness program. At the top left is the 'IT SECURITY AWARENESS' logo, and at the top right is the 'United Technologies' logo. A navigation bar contains links for HOME, ACTIVITIES, Q&A TOOL, RESOURCES, TRAINING, and FEEDBACK. The main banner features the text 'It's CYBER SECURITY AWARENESS MONTH 2013' in a stylized font. Below the banner are several interactive elements: a 'Help us baseline security awareness at UTC' button, a 'Phishing & Malicious Spam' video button, an 'EXPLORE THE INFOSEC GUIDES IN THE READING ROOM' button, a 'WHAT HAPPENS when you CLICK' button, a 'PLAY SPAM CATCHER' button, and a 'Try our crossword puzzle' button. The lower section includes an 'ALERTS' section with links to 'CryptoLocker Ransomware Infections' and 'Philippines Typhoon Disaster Email Scams and Phishing Attack Warning', a 'UTC Now Awareness Article Archive' link, and a 'SANS SECURITY TIP OF THE DAY' section with a list of tips. At the bottom, there is a 'HEADLINES BY FEEDBURNER' section and a 'SANS security' logo.

A Flash player that flips through a variety of banners highlighting new articles, videos, and games. These were updated on a weekly basis during October.

These buttons also changed weekly to highlight the campaign.

New alerts, weekly articles, and SANS security tips

# Phishing Game



**SPAM CATCHER**  
TEST YOUR SKILLS

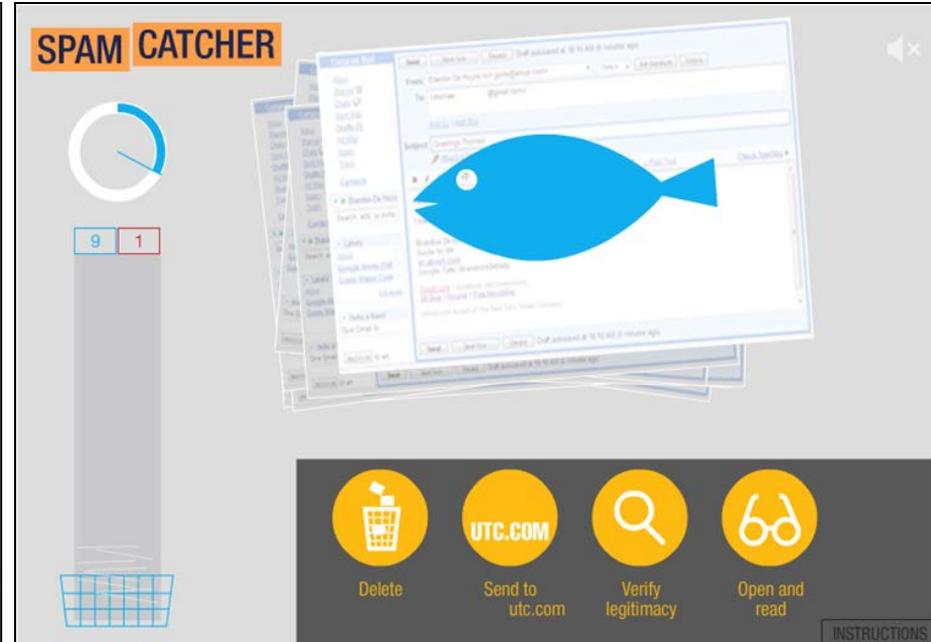
UTC receives 50 million SPAM emails per day. 98% are blocked. Some get through.

Help protect our systems.  
Know what to look for.  
Know what to do.

UTC IT Security

INSTRUCTIONS PLAY THE GAME

The banner features a dark blue background with a stack of email screenshots. One email prominently displays the word "SPAM" in large blue letters. A blue arrow points to the left, indicating the direction of the game's scroll.



**SPAM CATCHER**

9 1

Delete Send to utc.com Verify legitimacy Open and read

INSTRUCTIONS

The game interface is set against a light grey background. At the top left, a circular progress indicator shows a blue arc. Below it, a vertical grey bar contains a score of "9" in a blue box and "1" in a red box. A blue fish icon is positioned in the center, facing left. To the right, a stack of email screenshots is visible, with the top one showing a "Check for updates" button. At the bottom, a dark grey bar contains four yellow circular icons: a trash can, "UTC.COM", a magnifying glass, and the letters "bd". Below these icons are the labels "Delete", "Send to utc.com", "Verify legitimacy", and "Open and read".

This third party phishing game scrolled through a variety of different “emails,” where the users had to quickly determine whether it was spam, a phishing attempt, or a legitimate email.

# Scavenger Hunt

The screenshot shows a web application titled "SCAVENGER HUNT". At the top, there is a navigation bar with links for HOME, ACTIVITIES, Q&A TOOL, RESOURCES, TRAINING, and FEEDBACK. Below the navigation bar, the title "SCAVENGER HUNT" is displayed in a large, bold, serif font. Underneath the title, there is a form for entering the "Name/Team Name:" followed by a text input field. To the right of the input field is a "Go Scavenger!" button. Below this, there is a small paragraph of instructions: "Use the button to open a new browser window to search for the answers to all the scavenger hunt questions below. Then submit your answers to see if you can get into the high-score scoreboard." To the right of this text is a "View Top 20 Scores" link. The main content area is a table with three columns: "Points", "Question", and "Answer". The table contains ten rows of questions, each with a corresponding points value and a hint. At the bottom of the table, there is a "Submit Answers" button. Below the button, there is a note: "Top scores with Name or Team Names will be posted to results page for bragging rights!!".

Points	Question	Answer
10	SANS Institute issues monthly Security Awareness Newsletters called "OUCH". Find the title of the July 2013 issue.	<input type="text"/> Hint: (2 Words)
10	In a previous Security Awareness article on UTC Now titled "Security Awareness: Computer security tips and tricks" How many tips are listed that everybody should know how to do?	<input type="text"/> Hint: (1 Number)
5	From previous: If you have done the tips, type 'done' in this box.	<input type="text"/> Hint: (1 Word)
15	Find the UTC ePolicy website, click on 'Information Technology' in the Policy Type column, and type in the name of the first category under the UTC Policy Category column.	<input type="text"/> Hint: (4 Words)
15	Use the Search button on the ePolicy website to find the IT Policy document number (i.e. IT-00-000) that lists the controls regarding the use of 'shareware'.	<input type="text"/> Hint: (IT- -)
10	Find the section of the Corporate Policy Manual (CPM) discusses the protection of UTC data.	<input type="text"/> Hint: (1 Number)
15	Find the email address used to report spam or a phishing email.	<input type="text"/> Hint: (1 Email Address)
10	On the UTC IT Security home page, find what 'IRT' stands for.	<input type="text"/> Hint: (3 Words)
10	Find the topic of IT Policies listed in policy domain 11.	<input type="text"/> Hint: (2 Words)

Top scores with Name or Team Names will be posted to results page for bragging rights!!

The Scavenger Hunt allows users to learn about a few different websites and resources: the Security Awareness website, our IT Security homepage, and our IT Policies tool. Users can play in teams and then compete to find out who got the most correct answers.

# Videos



This year we had four different videos highlighting how each subject affects UTC. IT Security managers presented different viewpoints in a simplified manner to reach as many users as possible. These videos were also included in articles, and presentations.

# Q&A Tool

IT SECURITY AWARENESS  
UNITED TECHNOLOGIES CORPORATION

United Technologies

HOME ACTIVITIES **Q&A TOOL** RESOURCES TRAINING FEEDBACK

## Q&A Tool

Type Your IT Security Question Here

Submit!

ALL ( 139 ) GENERAL ( 47 ) EMAIL ( 20 ) INTERNET ( 8 ) MY COMPUTER ( 29 ) IT POLICIES ( 34 )

Nobody is doing anything about it.

- How is it possible for a phishing e-mail to install malware if you are not running under an administrator account, which most of us are not? 10/30/2013

Malware doesn't need admin rights to install. This is why it is so important that all users understand the risks of clicking on links in emails, pop-ups when browsing the Internet, etc.

- How is it that passwords can be guessed? Can't software be written that denies access after a set number of incorrect guesses? If not, why can't a "sleep" or "wait" type of command be programmed into our computers to slow the rate at which an automated attack can guess passwords? 10/30/2013

If a cyber-attacker is able to gain access to the encrypted password file they can run this through a password cracking program for as long as it takes to get a match. They don't need to try to guess a password by entering it into the account login screen. We also use the account lockout (until manually reset or for just a period of time, such as an hour) feature to defend against the casual attacker who is trying to just guess a password by entering it into the account login screen.

+ Why do I get much more spam through UTC than when we were Goodrich? 10/29/2013

+ Are there any plans to decouple the use of Java from our browser tools? Many of the tools we have use Java but with the increasing numbers of security issues it would seem like its use should be phased out 10/29/2013

+ I've read that Apple products are not as susceptible to viruses and other attacks. Why don't we use Apple products at UTC? 10/29/2013

+ How can I virus scan a thumb drive if I'm suspicious of the files it contains? 10/28/2013

The Q&A tool is a resource we've used for two years. Users put in questions anonymously. Questions are answered by our security team and subject matter experts.

# Reading Room

**IT SECURITY BUSINESS** **United Technologies**

HOME ACTIVITIES SERVICES RESOURCES TRAINING FEEDBACK

## READING ROOM

**INFOSEC GUIDES**

- AT&T Connect
- Backup
- Data Protection
- Email Attachments
- Email Phishing
- Email Spam
- Encryption
- Home and Hub
- IT Policies
- Malicious Software
- POP
- Passwords
- Patching
- Physical Security
- Smart Phone Security
- Software Licensing
- Suspicious Incident
- Traveling
- USB Drives
- Using Secure Websites
- Voices
- Wireless

**ARTICLE ARCHIVE**

**UTC LINKS**

**EXTERNAL LINKS**

### Email Spam (including malicious spam)

Spam used to simply be unwanted commercial emails. Annoying and inconvenient, but nothing more. While the total number of spam messages are decreasing over time the percentage that is suspected of being malicious is increasing. This so called "malicious spam" is much more concerning. Malicious spam emails include links or attachments which when clicked/opened can lead to the installation of malware (viruses) on your computer, allowing a hacker to steal your information and company information. Similarly, phishing emails are attempts by cyber criminals to gain your trust to obtain personal or company information including passwords & credit card information.

The UTC IT Shared Services Messaging Team works diligently with our suppliers to block all spam and unsolicited email from entering the UTC's mail system. An average of 50 million messages are sent to UTC on a daily basis, with occasional peaks of 100 million. More than 90% of these messages are identified as spam and blocked from entering our email system. Some spam and phishing emails do get through. Everyone needs to be vigilant to this threat. The UTC workforce is critical to our success in combating spam and phishing.

Here are some recent examples of malicious spam and phishing emails:

#### Tips for @ Work

- You should send any suspicious emails with links or attachments in an email to Do this by highlighting the suspicious message in your inbox then click Ctrl + JH + F.
- You can make a critical difference: suspicious emails sent to the spam mailbox by UTC users have resulted in the identification (and subsequent elimination) of new malware created by cyber attackers and unknown to anti-malware vendors.
- Don't respond to spammers (it will only confirm that your email is an active one).
- Be very careful about sites that allow you to unsubscribe. Unless they are from legitimate companies that you may have signed up on their mailing list, they often are a means to collect more active email addresses.
- Don't use your work email for mailing lists or websites. It's best to create a separate email address at home just for registering with on websites.
- If you see the same email often, you can write a rule in Outlook to automatically delete/move it (<http://www.microsoft.com/office/outlook/help/makeanemailrule.aspx>).
- If you receive a significant amount of spam (defined as consistently more than 15 messages a day), call the help desk.
- There are times when a seemingly suspicious email could be valid. For example, if you receive an email from your bank about unusual activity on your account you might contact your bank via a different communication method - the telephone, for example - and confirm whether this is valid or not.
- The IT Shared Services Messaging team have additional spam reference materials and guidance [here](#).

#### Tips for @ Home

- Use an email service that provides spam filtering
- Create a separate email address for registering on websites
- There are times when a seemingly suspicious email could be valid. For example, if you receive an email from your bank about unusual activity on your account you might contact your bank via a different communication method - the telephone, for example - and confirm whether this is valid or not.
- Do not use your work computer to check your home email when you are not connected to UTC
- Be careful of "hand this to everyone you care about" and anything else that is mass forwarded. If you must respond, use BCC for all recipients. Tell anyone sending this type of traffic to you to use BCC. This will prevent your email address from being harvested if anyone else the mail is forwarded to gets a virus.

#### Links

- [Spam, Phishing, Malware & Other Malicious Attacks](#)
- [Our one page guide to Outlook](#)
- [UTC's spam test interface](#)
- [ITC - Spam](#)

The Reading Room is filled with articles showing users how to be safer at work and at home. Examples and links are also included.

# Crossword Puzzle

**IT SECURITY AWARENESS**  
UNITED TECHNOLOGIES CORPORATION

**United Technologies**

HOME    ACTIVITIES    Q&A TOOL    RESOURCES    TRAINING    FEEDBACK

### Crossword

**Across**

- 2. Uses virtual 'bait'.
- 5. Software that compromises security on a user's computer.
- 7. Used with a user ID to access an application.
- 8. Protects data by making it unreadable.
- 9. Should be activated and password protected when an employee is not at their desk.
- 10. Protects UTC network from unauthorized access.

**Down**

- 1. Communication medium targeted for phishing and social engineering attacks.
- 3. Web address should start with this when submitting sensitive information online.
- 4. Type of UTC data which should be protected
- 6. Software which should be updated regularly to protect against computer viruses.

**Cheat Letter**    **Cheat Solution**

After the user goes through the reading room, they can use their new knowledge and vocabulary in the crossword puzzle.

# Awareness Quiz

**?? Awareness Quiz??**

Will you be a "Best Practice Role Model" or a "Security Fail"?  
Test your security knowledge by taking the 2013 awareness quiz.

1. What is the number one method that external attackers use to gain unauthorized access to the UTC network?
  - Password cracking
  - Email phishing
  - Packet sniffing
  - Dumpster diving
2. True or False: It is ok to connect your personal mobile phone to your UTC computer.
  - True
  - False
3. What kind of software can be installed on your UTC computer?
  - Software which has a license that allows for business use, is approved by the Business Unit IT management and is in compliance with license terms
  - File sharing software
  - Games
  - Personal tax software
4. What is a good way to remember your password?
  - Use the same password for all of your accounts
  - Click on 'remember my password' every time you log into an account
  - Associate your password with a phrase
  - Write your passwords on a sticky note next to your computer
5. How can you protect UTC data when you leave your desk during the day?
  - Lock your computer with the combination of the Windows start menu key and the letter "L"
  - Take any keys or access badges with you
  - Remove files or notes from your desk and store in a locked drawer
  - All of the above
6. Which is an example of a good password?
  - 12345678
  - Pa55w0rd
  - mydogfluffy
  - 5P0ky13Z
7. Which is NOT a good way to protect UTC data on a USB drive?
  - Encrypt your USB drive
  - Keep USB drives in a safe place
  - Use your USB drive on someone else's computer
  - Use password protection on your USB drive
8. What is the best way to protect your information when using Wi-Fi to connect to the internet?
  - You don't need to. Wi-Fi is completely secure.
  - Connect to a peer-to-peer network.
  - Use IPsec encrypted VPN to connect to the UTC network to ensure data is encrypted and protected

The quiz asks eight randomized questions for a user to learn how secure they really are. Afterwards, they get a score, the correct answers, and a chance to retry with different questions.