

City of Stamford
Technology Department

Employee Orientation



CITY OF
STAMFORD

innovating since 1641

Gaining Access to the Network

- Your direct supervisor must complete a *Network Access Form*, available from the City Intranet: *www.Staminet.org*
 - Email
 - Internet Access
 - Security Groups and workshare permissions
 - Map the “H” drive
 - Employee intranet (<http://CityNet>) under Employee Forms
 - Password Manager: www.Stamfordct.gov/password

Privacy and the Network

- Read the Technology Policy
 - ***“No Expectation of Privacy”***
- Do not store personal pictures, photos, music, “Funny” videos or other non-work items on your computer or the network
- The Technology Department will occasionally sweep the network for these and other items such as installed software and browser history
- As a public entity we are subject to the Freedom of Information Act

Getting Help

- **City Employees and BOE Administration**
 - Call the Help Desk at 977-4936
 - Email HelpDesk@Stamfordct.gov
- **School employees**
 - Contact the technology coach or designated person at your school
- **Other locations such as Police and Fire**
 - Contact your supervisor

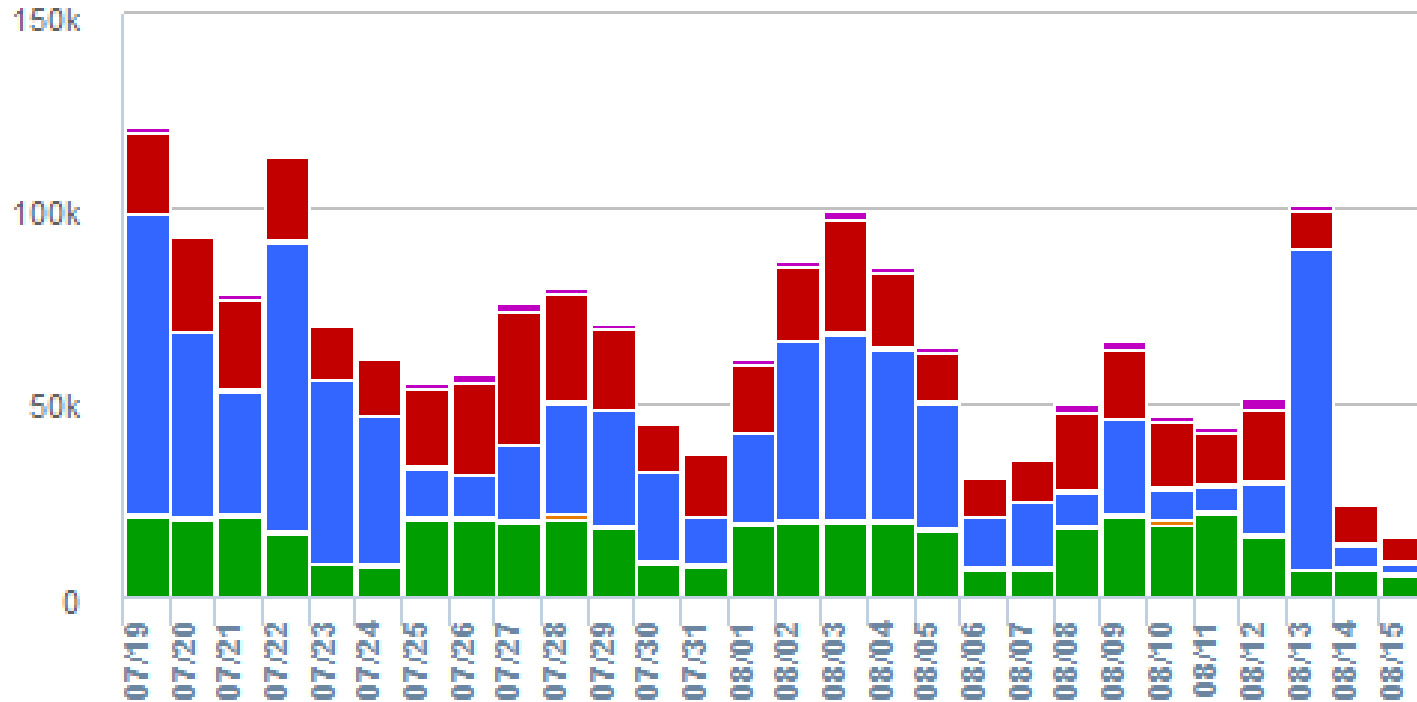
Email

- Your Email address will be:
 - *username@StamfordCT.Gov*
 - Accessible from the intranet
 - Webmail: www.StamfordCT.gov/mail
- **If you wouldn't want it in the front page of the news paper it shouldn't be in your email.**
- We archive all email before it is delivered to your inbox
- Treat your email like an unlisted number
- **DO NOT** use your City email for things like Facebook, Shopping updates or other non-City purposes.
- Report suspicious email to the Help Desk at HelpDesk@Stamfordct.gov Don't
- keep mail in your Deleted Items. There is a 30 day retention policy.

Email Statistics

Daily Mail Statistics [inbound]

Help



Blocked: Bad Recipient Blocked: Spam Blocked: Virus
Rate Controlled Quarantined Allowed: Tagged Allowed

Think Before You Click

- The Technology will **NEVER** ask you for your password. If you receive an email asking for your user name and password to “reset your account” it is spam!
- Be wary of unsolicited emails and attachments. If you don't know who it is from or weren't expecting it, it is probably SPAM.
- If the email looks suspicious **DO NOT** click on any links!
- Don't use the “Unsubscribe” link of a SPAM email. IF it is an annoyance you can create a rule in Outlook to send them to the Deleted Items
- Most SPAM can just be deleted

Internet Access

- Our internet access is filtered and monitored
- Treat it as a business tool.
- The Technology Department, as an agent of the City, may monitor any and all communications, including browser history
- Some sites that have a lot of advertising have been known to have “infected content”
- Do not download and install programs from the internet

Social Engineering Red Flags

FROM

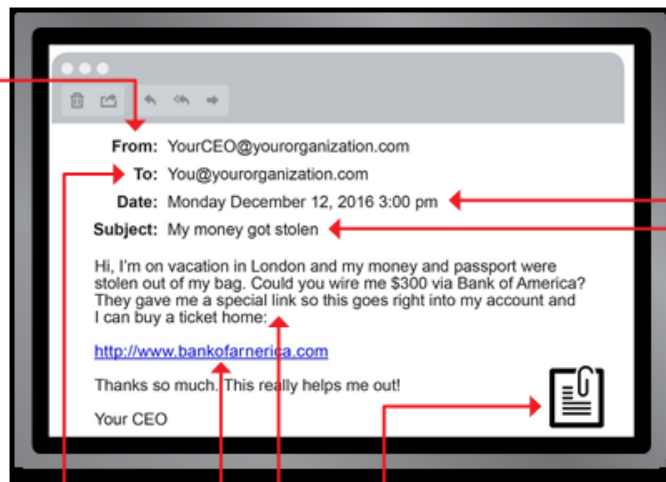
- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

TO

- I was sent on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- When I hover my mouse over a hyperlink that's displayed in the email message, but the link-to address is for a different website. (This is a big red flag.)
- I received an email that only has long hyperlinks with no further information, and the rest of the email is completely blank.
- I received an email with a hyperlink that is a misspelling of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- I don't receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

SUBJECT

- I don't get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

ATTACHMENTS

- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

CONTENT

- Under asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

Standard Software Applications

- The Technology Department is responsible for maintaining a stable and secure computing environment
- Standard Software
 - Microsoft Office
 - Adobe Reader
 - Symantec Anti-Virus
 - H.T.E, Kronos, Ceridian, Starbase or other enterprise software as appropriate
 - **Appropriately licensed software for your job**
- Contact the Technology Department if you need a particular software package that is not a standard.

Non-Standard Software Applications

- Third Party Screen Savers
- Internet Games
- Peer-to-Peer file sharing
- Other personal software
- All of these present either a technical threat to the global computing environment or a conflict with our established software.
- If you place a service call and the source of the problem is found to be a non-standard software application the Technology Department may opt to format your machine.

Non-Standard Computers

- You may NOT bring in you personal computer and plug it into the City or Education network.
- Personal mobile devices such as iPads and tablets can use the COSGuest network for internet access
- The Technology Department does not support Apple computers or personal smart phones.