# Easy Action Toolkit for Employees and Managers

## Find out... *What's the Big Deal*!

| Safe Workplace | | | | |
|---|---|---|---|---|
|  Building Access Cards |  Building Evacuations | |  Personal Safety Threats |  Access to Work Buildings / Areas |
| **Safe Saving, Storing, Sending & Receiving** | | | | |
|  Email Signatures |  Emailing Sensitive Information |  Emailing to Home or Personal Accounts |  Email (Think First) |  USB Keys |
|  Phishing – Clicking on Links |  Phishing – What to Consider |  Phone Scams |  Mailing Sensitive Documents |  Clean Desks |
| **Safe Equipment** | | | | |
|  Securing Computers (In the Office) |  Securing Computers (Out of the Office) | |  Personal Devices at Work |  To Do: End of Workday |

# Contents

***What's the big deal if…***

***…I lend my ID/Access card to a colleague?***

| **Why it is a big deal** |
|---|
| • You will be held responsible as the owner of the ID/Access card if an incident occurs (e.g. loss of the card, access to restricted areas) |
| **Scenario** |
| Your co-worker Phil forgot his ID/Access card and knows that you're going to a two-hour meeting off-site. He asks to borrow your card. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Refuse because your card is for your use only<br>• Option 2: Give Phil your ID/Access card and grab it when you get back<br>• Option 3: Tell Phil to ask another colleague |
| **Explanation** |
| • Option 1 is the correct option<br>• By not lending your ID/Access card you are respecting the privileges and use of the card assigned to you |
| **Key take-aways** |
| • You must never lend your ID/Access card to anyone<br>• You must wear your ID/Access card so it is visible – each day, all day long - while at work<br>• If you forget your ID/Access card, tell your manager/team leader who will make temporary arrangements for you<br>• If you lose your card or if it is stolen, immediately advise your manager/team leader, and complete the Security Incident Report |
| **More information** |
| • Physical Security |

***What's the big deal if…***

## *…I don't go to our team's designated meeting area during an evacuation?*

| **Why it is a big deal** |
|---|
| • Your manager/team leader and colleagues will not know that you got out of the building and will not be able to account for you<br>• You will miss any information provided and/or instructions to follow |
| **Scenario** |
| You're leading a meeting when alarms sound, indicating that you must evacuate. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Exit the building and grab lunch as it's almost noon<br>• Option 2: Finish the meeting quickly, then go to your designated meeting area<br>• Option 3: Secure your work materials and go immediately to your designated meeting area |
| **Explanation** |
| • Option 3 is the correct answer<br>• Always go immediately to your team's designated meeting area. In doing so, your manager/team leader and colleagues will know that you are safely out of the building and can provide you with information and further instructions |
| **Key take-aways** |
| • Always know the location of your designated meeting area<br>• When the alarm sounds for an evacuation, leave the building in a calm and orderly manner and go directly to your designated meeting area<br>• Do not cause any unnecessary delays while exiting (e.g. texting, stopping to talk, waiting for a colleague to catch up with you, etc.)<br>• Follow the instructions of your manager/team leader or your Building Emergency Organization (BEO) member |
| **More information** |
| • Employee's Guide to Emergency Situations<br>• Building Emergency and Evacuation Teams Toolkit |

***What's the big deal if…***

## *…I don't report an incident involving a threat to my personal safety?*

| **Why it is a big deal** |
|---|
| • First and foremost, you matter! Not reporting an incident immediately could put your well-being and others at risk<br>• Second, ESDC is committed to ensuring that every employee is protected from workplace violence. If a situation occurs that threatens your personal safety or the safety of others, the Department needs to know in order to respond immediately and act accordingly |
| **Scenario** |
| After a tense phone call, an EI client has threatened to come to your office and "give you what's coming to you". What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Inform your manager/team leader and fill out the Security Incident Report, which will then be sent for investigation<br>• Option 2: Do nothing. You know that they won't follow through<br>• Option 3: Tell your manager/team leader that you aren't feeling well and go home immediately |
| **Explanation** |
| • Option 1 is the correct option<br>• When a situation of a threatening nature occurs, you **must** report it immediately to your manager/team leader and complete the Security Incident Report. These procedures have been put in place to assist the Department with the safety of all employees |
| **Key take-aways** |
| • You matter!<br>• Don't be afraid to report situations that could pose a risk to the safety of you or others<br>• Your manager/team leader will respond and get you the support you need; complete fact gathering; and implement any actions required<br>• The Department will not be able to help you or be able to respond to the situation if it is not reported. Note: In the case of an immediate threat call 9-1-1 and advise your manager/team leader |
| **More information** |
| • Guideline - Personal Safety in the Workplace<br>• Security Incident Report – ADM3061 |

***What's the big deal if…***

## *…I hold the door open for someone behind me?*

| **Why it is a big deal** |
|---|
| • You don't know if the individual is there legitimately or if he/she is a thief or a personal threat<br>• You could put your safety, and your colleagues' safety, at risk<br>• You could put departmental information and assets at risk of damage or theft |
| **Scenario** |
| You arrive on your floor and notice a few individuals standing at the entrance door to your work area. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Use your access card to enter your work area and proceed to your desk<br>• Option 2: Unlock the door with your access card and then hold the door open, so everyone can enter your work area<br>• Option 3: Use your access card to enter your work area and make sure that the door closes and locks behind you |
| **Explanation** |
| • Option 3 is the correct answer<br>• Using your access card and ensuring that the door locks behind you sends a clear message that others must enter using their own access cards |
| **Key take-aways** |
| • Holding the door open for others because it's polite can put those who work in a building, as well as the information and assets on the premises, at risk<br>• Everyone who has authorized access to departmental buildings is provided with their own access card for entry<br>• There are processes in place to allow temporary authorized entry into work areas for legitimate visitors |
| **More information** |
| • Video on Tailgating<br>• Physical Security |

***What's the big deal if…***

## *…I don't use the standardized signature block?*

| **Why it is a big deal** |
|---|
| • The recipient could very likely delete your e-mail, thinking it is spam or report it as a phishing attack<br>• TBS requires that you use a standardized signature block for identification and to reduce questions about credibility of the e-mail<br>• A new e-mail system is coming to the Department that will standardize all e-mail addresses. Your signature block will be the only way for someone to identify what department you work for |
| **Scenario** |
| You've been told that your e-mails are being deleted and not read because it's not clear who they are from. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Use the standardized signature block as outlined by TBS<br>• Option 2: Create your own customized signature block which includes a thought-of-the-day<br>• Option 3: Sign the e-mail with "Cheers" and your name |
| **Explanation** |
| • Option 1 is the correct option<br>• You must follow the official signature block from TBS to ensure your e-mails are properly identified and not mistaken for phishing<br>• The TBS Standard for e-mail signatures includes (in bilingual format, always):<br>Name<br>Title, Branch<br>Department / Government of Canada<br>E-mail / Telephone / Teletypewriter |
| **Key take-aways** |
| • To avoid confusion, use a standardized signature block on all your e-mails |
| **More information** |
| • Signature block template<br>• TBS Standard on Email Management |

## *What's the big deal if…*

## *…I e-mail sensitive information?*

| **Why it is a big deal** |
|---|
| • It is important to know the sensitivity level of the information you are e-mailing. Sensitive information that you send could be at risk if it is lost, intercepted or sent to the wrong person. |
| **Scenario** |
| Your colleague in another department requested a document containing a date of birth and a Social Insurance Number (SIN). What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Encrypt the document using Entrust, then e-mail it<br>• Option 2: Put the SIN in the e-mail Subject line to alert your colleague<br>• Option 3: E-mail the document as is |
| **Explanation** |
| • Option 1 is the correct choice – an e-mail containing a SIN and another piece of personal information is Protected B and must be encrypted.<br>• The key is to know what constitutes Protected B. An email that contains one piece of personal information such as a SIN is not considered Protected B by itself and therefore it does not have to be encrypted.<br>• However, it is a good practice to take preventative measures and encrypt sensitive information before sending. But, when you send Protected B information outside the departmental firewall, it must been encrypted using Entrust. |
| **Key take-aways** |
| • Think about the information you are sending, its sensitivity level, and ensure it is properly safeguarded.<br>• You should not put names, SINs, Personal Record Identifier (PRI), date of birth or other personal information in the Subject line of e-mail messages.<br>• When you send an e-mail outside the ESDC e-mail system, we can no longer manage the security of the information sent in the e-mail.<br>• Additionally, you should make sure that the receiver has a "need-to-know" the information.<br>• The receiver must also have Entrust to be able to open the document. |
| **More information** |
| • Sending Sensitive Information via E-mail<br>• Transmitting Information Securely<br>• How to Encrypt a Document (PDF, 178 KB)<br>• How to Send an Encrypted Email (PDF, 203 KB)<br>• Handling of Information and Required Safeguards |

***What's the big deal if…***

## *…I e-mail work files to my home computer to work on?*

| **Why it is a big deal** |
|---|
| • You're putting the confidentiality of the information at risk – the e-mail could be lost, intercepted, or accidentally sent to the wrong person<br>• You cannot guarantee the security of the files when they're in transit or, when they're on your home computer |
| **Scenario** |
| You need to complete a report that is due tomorrow morning, but you won't be able to finish it at work so you want to take it home. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: E-mail it home. It'll be okay since you'll just do it this one time<br>• Option 2: Get approval from your manager and borrow the appropriate department-issued equipment (e.g. encrypted USB key or laptop)<br>• Option 3: Password protect the document, then e-mail it home |
| **Explanation** |
| • Option 2 is the correct choice – your manager should get the right equipment for you<br>• E-mailing work files to your personal e-mail account is a security violation<br>• Password protecting documents does not provide enough protection. Passwords can easily be cracked |
| **Key take-aways** |
| • If you need to work from home, then talk to your manager. The appropriate devices will be issued to you (i.e. laptop, encrypted USB key)<br>• It is a security violation to e-mail work related documents to your home computer |
| **More information** |
| • Taking Work Home – A Decision Making Flowchart<br>• Network Use Directive (see section 5.9) |

***What's the big deal if…***

## *…I Reply All to an e-mail without checking the recipient list?*

| **Why it is a big deal** |
|---|
| • You could potentially disclose sensitive information to people who are not supposed to have it<br>• You could cause confusion, as recipients won't understand why they are getting your e-mail<br>• You could crash the department's electronic network |
| **Scenario** |
| You received an e-mail as part of a large distribution list and you need to provide a response. What should you do first? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: BCC everyone on your reply. This will ensure further Reply All's don't occur.<br>• Option 2: Reply All. There must be a reason why everyone was on the original list.<br>• Option 3: Think about why you were on the email list and decide if Reply All is what you should be doing. |
| **Explanation** |
| • Option 3 is the right choice<br>• The BCC field prevents recipients from replying to everyone, but take the time to consider if everyone needs to know your response<br>• Reply All should only be used if everyone needs to know your response AND the recipients need to be able to reply to everyone |
| **Key take-aways** |
| • Check the recipient list before replying to any e-mail<br>• Reply All with any distribution list should be used with caution<br>• Be aware of your obligations as it relates to the Network Use Directive |
| **More information** |
| • ESDC Network Use Directive |

***What's the big deal if…***

## *…I use my own USB key for work purposes?*

| **Why it is a big deal** |
|---|
| • If you lose/misplace it, you have also lost/misplaced the (department's) information on it<br>• ESDC policy states that for work purposes all employees must use a department-issued device |
| **Scenario** |
| You need to take electronic versions of some files to a meeting tomorrow. You think about getting a department USB key, but quickly realize you don't have enough time to get approved for one. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Use your own USB key because you've never had a problem with it before<br>• Option 2: Go buy a new USB key, that way you know it's safe<br>• Option 3: Email the files to the meeting chair or take them on a departmental laptop |
| **Explanation** |
| • Option 3 is the right choice<br>• Sending the files by email is the easiest way, as long as they're not classified above Protected B. If you have a department laptop, you can take the files on that<br>• Even though you've never had a problem with your personal USB key before, it doesn't mean that it's safe to use for work-related information<br>• Brand new USB keys that you buy from a store can be tampered with during production, so even though you think it's safe, it might not be. It can also be lost or misplaced |
| **Key take-aways** |
| • You must always use department-issued devices (laptops, USB keys) to transport department information<br>• You may only connect USB devices that are department-issued to the network |
| **More information** |
| • Portable Storage Devices<br>• Approved Portable Devices |

***What's the big deal if…***

***…I click on that link in a suspicious e-mail?***

| **Why it is a big deal** |
|---|
| • You may install a virus, which puts your computer and the information on it at risk. This puts the Department at risk<br>• You may launch spyware that allows a cybercriminal to steal your password. This password may be used to access other information on ESDC's electronic network<br>• This could lead to: loss of information, identity theft, network breaches, loss of client confidence, and/or financial gain for the cyber criminal |
| **Scenario** |
| At 4:48am you received an e-mail saying your computer may have a virus. It asks you to click on the link and enter your username and password so the IT branch can run a virus scan. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Delete the e-mail<br>• Option 2: Click the link and enter the information<br>• Option 3: Report it online to the National Service Desk (using the fishhook icon) |
| **Explanation** |
| • Option 3 is the correct answer<br>• If an e-mail is suspicious to you, especially if it asks for personal information (e.g. password, username), report it to the National Service Desk |
| **Key take-aways** |
| • Open e-mails from unknown sources with extreme caution<br>• If it is at all suspicious, don't take a chance. Do not reply, do not click on any links and do not open any attachments. Report it online to the National Service Desk, and then delete the e-mail |
| **More information** |
| • Video: Put a HALT to Phishing |

***What's the big deal if…***

***…I don't know what a phishing e-mail looks like?***

| **Why it is a big deal** |
|---|
| • You're putting our department's electronic network at risk if you get tricked into clicking on an infected link or attachment. You could accidentally download spyware or malware |
| **Scenario** |
| You receive an e-mail with the subject line "Urgent Matter" and there's a link to a PDF file. It might be about that new contract you're working on, but you're aware it could be fake. What clues do you look for to determine if it's a phishing e-mail? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Time stamp, signature block, spelling and grammatical errors, generic greeting<br>• Option 2: Subtle changes to e-mail domain names<br>• Option 3: Hover your mouse over the link to see the true path of URL |
| **Explanation** |
| • Options 1, 2 and 3 are right! These are just some of the clues that an e-mail is fake<br>• You need to examine all of these components together. If something is off, then report the e-mail online by clicking on the fishhook icon on the National Service Desk homepage |
| **Key take-aways** |
| • Phishing e-mails are one of the most common methods that cybercriminals use to steal information, so you need to know how to recognize them<br>• Open e-mails from unknown sources with extreme caution. Use HALT to help you determine if it is a legitimate e-mail<br>• If the e-mail seems fishy to you, it probably is! Do not reply, do not click on any links, and do not open attachments. Report it online to the National Service Desk, and then delete the e-mail<br>• If you think that the e-mail might be real, but you're unsure and don't want to delete it prematurely, verify the sender's e-mail address or telephone number through another method (e.g. GEDS, Outlook Directory). Then call or send them a new e-mail and ask if the message was legitimate |
| **More information** |
| • Put a HALT to Phishing<br>• Spam and Phishing |

***What's the big deal if…***

***…I don't recognize the signs of phone phishing?***

| **Why it is a big deal** |
|---|
| • You are likely to fall for a phone phishing attack, and give cybercriminals the information or the means they need to gain access to our electronic network. This puts Canadian citizens' information at risk |
| **Scenario** |
| The "IT Service Team" calls to say your computer is infected with a virus. The agent wants to know what type of anti-virus software you have and asks for remote access immediately, so they can clean your machine before the virus infects everyone's computer. What are the clues that this is a phone phishing attempt? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: The agent asked for remote access to clean your computer<br>• Option 2: The agent asked questions about what anti-virus software is installed on the computer<br>• Option 3: Used fear to motivate you to accept their help |
| **Explanation** |
| • All the options are clues that this is phone phishing<br>• Somebody from the Department's IM/IT National Service Desk will never ask you what software you have – they already know<br>• The National Service Desk does not require remote access to clean your computer of a virus |
| **Key take-aways** |
| • Do not answer any suspicious questions regarding the Department's computer system<br>• Do not give remote access to your computer unless you're sure it's legitimate (legitimate requests come from the National Service Desk or a resolver group as a result of a service request from you)<br>• When in doubt, hang up and tell your team leader/manager as soon as possible. Your team leader/manager must then contact the Regional Security Office to report the incident<br>• Don't rely on your phone's caller ID. Phone numbers can be spoofed |
| **More information** |
| • Voice Phishing |

***What's the big deal if…***

## *…I mail sensitive documents the same way as I would a birthday card?*

| **Why it is a big deal** |
|---|
| • The envelope might be inadvertently opened by someone who should not see its contents<br>• That 'someone' now has sensitive information, including potentially personal information that they are not entitled to have<br>• This could lead to fraud, identify theft and/or a misuse of that information |
| **Scenario** |
| During a file investigation, a Canada Revenue Agency (CRA) agent asks for a hard copy of a client's file that contains Protected B information. Your office's secure fax device has been sent for repairs. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Wait until the secure fax device has been repaired and returned<br>• Option 2: Double-envelope the client's file and mail it to CRA<br>• Option 3: Use regular fax to send the information to CRA |
| **Explanation** |
| • Option 2 is the correct answer<br>• When using a double envelope, the outer envelope does not advertise or draw attention to the sensitivity of the information contained within<br>• If it is opened inadvertently at CRA, there is another envelope inside that lets the individual know that contents are sensitive, and should be forwarded to the right person |
| **Key take-aways** |
| • Always use the correct safeguards and guidelines for mailing sensitive information<br>• When using double envelopes, mark the inner envelope with the appropriate security marking (e.g. Protected B). This identifies the sensitivity level to the addressee and helps them to apply the appropriate safeguards for its handling |
| **More information** |
| • Information Classification Guide<br>• Handling of Information and Required Safeguards |

***What's the big deal if…***

***…I leave files on my desk or open on my computer?***

| **Why it is a big deal** |
|---|
| • Anyone who passes by your desk could see information that they are not supposed to see<br>• That information could be copied, changed or taken from your desk or computer<br>• You put yourself in a position of having to explain why information, for which you were responsible, has been lost, copied or changed if there is a security incident or investigation |
| **Scenario** |
| You are working at your desk on two client paper files that are Protected B. Your manager asks you to join a meeting with the director immediately. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Flip the papers upside down on your desk and go to the meeting<br>• Option 2: Lock the two files in a cabinet and also lock your computer<br>• Option 3: Leave the files face up on your desk since you work in a restricted zone you feel confident that doing this won't be a problem |
| **Explanation** |
| • Option 2 is the correct answer<br>• Locking the paper files in a cabinet protects the clients' information from any unauthorized access<br>• Locking your computer protects against any unauthorized access and/or modification to electronic files (including e-mail) |
| **Key take-aways** |
| • You don't want to be responsible for information being lost or getting into the wrong hands, especially that which is sensitive or personal<br>• Always safeguard information (paper and electronic) in your custody when you are not at your desk<br>• Information that is not secured is vulnerable |
| **More information** |
| • Clean Desk Guidelines<br>• Information Classification Guide<br>• Handling of Information and Required Safeguards |

***What's the big deal if…***

## *…I don't secure my electronic devices when I leave my desk?*

| **Why it is a big deal** |
|---|
| • Someone could steal or tamper with it<br>• Someone could steal or tamper with the information that is on it (or on our ESDC electronic network) |
| **Scenario** |
| Returning from a meeting, you notice that you left your BlackBerry on your desk. What should you have done before leaving your desk? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Nothing. You trust your colleagues sitting near you<br>• Option 2: Lock your BlackBerry in your cabinet or take it with you<br>• Option 3: Turn off your BlackBerry because then it's okay to leave behind |
| **Explanation** |
| • Option 2 is the correct answer – securing your devices is crucial in maintaining the security of the equipment and the information on them<br>• Your colleagues aren't the only ones who have access to your desk – clients, visitors, and building personnel also need to be considered<br>• Shutting down your devices doesn't protect them from theft |
| **Key take-aways** |
| • Take the time to secure your electronic devices, even if you're only stepping away for a minute<br>• Protect your devices and protect the information on your devices |
| **More information** |
| • Workspace and Desktop Security |

## *What's the big deal if…*

## *…I use my personal computer to work offsite?*

| **Why it is a big deal** |
|---|
| • Your personal computer does not have the same security protection as the ESDC electronic network<br>• If the device is lost, the information on it (that belongs to the Department and Canadians) is lost<br>• If somebody else in your home has access to the computer, they have access to information that they should not<br>• Under no circumstances should you e-mail work information from home to the office (or vice versa) as this creates even greater security risk |
| **Scenario** |
| You planned to work from home tomorrow, but on the way home you realize you forgot your work laptop at the office. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: E-mail a colleague and ask them to send the files you need to your personal account<br>• Option 2: Go back to the office and get your work laptop<br>• Option 3: Call your manager and ask for permission to use your personal computer |
| **Explanation** |
| • Option 2 is the correct answer – even though it means an extra trip into the office<br>• Your personal computer is not a department authorized device, and therefore should not be used when handling work information<br>• Your manager should not give you permission to use your personal computer for work purposes<br>• The exception to this is if you have been authorized to use AppGate for remote desktop access, then you can use your personal computer for work purposes |
| **Key take-aways** |
| • You have a responsibility to protect information whether you're working onsite in an office or offsite<br>• Work that you do offsite must be done either on a department authorized device using a Virtual Private Network (VPN) or on your personal computer using AppGate |
| **More information** |
| • Laptop Security<br>• VPN and Remote Access |

***What's the big deal if…***

## *…I connect my personal cell phone to my work computer?*

| **Why it is a big deal** |
|---|
| • Your personal cell phone (or iPod or tablet or other personal device) could be infected with malware or a virus. When you plug that in, you are connecting to the ESDC electronic network and potentially introducing the malware/virus to our network |
| **Scenario** |
| You're expecting an important personal phone call, but your cell phone is low on battery. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Charge it by connecting it to your computer<br>• Option 2: Charge it using an electrical outlet<br>• Option 3: You can't charge it at work |
| **Explanation** |
| • Option 2 is the correct answer. To charge your personal devices, you must use the electrical outlets<br>• This applies to all your personal devices (e.g. music players, digital cameras, tablets, e-readers), not just cell phones |
| **Key take-aways** |
| • You may only connect authorized devices to the network because they have the necessary security features to protect departmental information<br>• You are not allowed to connect your personal devices to your workstation, your laptop, or the network<br>• Departmental computers are scanned to ensure no unauthorized USB devices are connected |
| **More information** |
| • Approved Portable Media<br>• Portable Storage Devices Directive |

***What's the big deal if…***

***…I leave my computer on all night OR I shut it right off at the end of the day?***

| **Why it is a big deal** |
|---|
| • Software upgrades and important security patches are happening at night while you sleep<br>• These won't happen if equipment is shut down or just identified as 'away'<br>• Software upgrades allow employees to have the best that technology has to offer in ESDC<br>• Security patches include anti-virus updates and scans to ensure the safety of the ESDC electronic network and all of the information on it |
| **Scenario** |
| You're preparing to leave on a 3-week vacation. You want to be as "green" as possible and conserve energy, so you think about powering off your computer. What should you do? |
| **Possible actions (vote on the correct answer)** |
| • Option 1: Lock your computer(Ctrl-Alt-Del-Enter)<br>• Option 2: Restart (Start-Shut Down-Restart-Ok)<br>• Option 3: Power down (Start-Shut Down-Ok) |
| **Explanation** |
| • Option 2 is the correct answer<br>• If you're concerned about the being green and not wasting energy, technologies are being investigated so that in the future, you will be able to power off your machine at night |
| **Key take-aways** |
| • You must follow the proper procedure of "Start-Shut Down-Restart-OK" every night<br>• Even on Fridays and even on the last day before a vacation!<br>• Not having the most recent software updates, anti-virus programs, and security patches leaves your computer vulnerable to attack<br>• If you work offsite, do not shut down or restart. You must only log off, in order to keep your VPN connection alive to allow for patches and software updates |
| **More information** |
| • Security on iService |