mtiic
MINISTRY OF TRADE, INDUSTRY,
INVESTMENT AND COMMUNICATIONS

TTBizLink
Business Made Easy

Your Guide to Information Security Awareness on TTBizLink

www.ttbizlink.gov.tt

Information security is everyone's responsibility.

Be an ambassador for awareness and change.

published by
THE MINISTRY OF TRADE, INDUSTRY, INVESTMENT AND COMMUNICATIONS
SINGLE ELECTRONIC WINDOW (SEW) - TTBizLink
Level 9 Nicholas Tower, 63-65 Independence Square, Port of Spain
Republic of Trinidad and Tobago   Help Desk: 800-4SEW or 800-4739
Fax: 1 (868) 623-5156   E-mail: support.ttbizlink@gov.tt

Contents

Did you know?

Safeguarding information is important to everyone in all aspects of daily life. We each have a responsibility to protect information placed in our remit. The same responsibility applies to protecting all information involved in the TTBizLink initiative.

Each of us plays an important part in protecting our information and the information entrusted to us by our citizens, business partners, stakeholders and employees.

Just like a chain, security is only as strong as its weakest link. We are part of the chain. Let's keep it strong.

The TTBizLink website - **www.ttbizlink.gov.tt** - also has valuable information on various pieces of legislation that provide for information security. For example, under the menu heading Tariff and Legislations on the left hand side of the home page can be found the Data Protection Act. No. 13 of 2011 which is an Act to provide for the protection of personal and private information. Part I, Section 7 to 18, 22, 23, 25 (1) and 26 and section 28 of Part II of this Act have been enacted. Also to be found here are the Computer Misuse Act-11.17 and the Interception of Communications Act 2011.

What is information security?

Information security is how we protect one of our most valuable assets - our information. The goal of information security is to preserve the confidentiality, integrity and availability of information assets, to ensure business continuity and to minimize business damage by preventing and reducing the impact of security incidents. Risks will be greatly mitigated by the implementation of information security measures. Such measures would require organization-wide security awareness, management support and commitment to the TTBizLink integrated security framework.

Why is this important?

Failure to secure our information can significantly impact on our brand and reputation. Remember, security is at the core of who we are and what we do. It plays a key role in our promise to our stakeholders. This is why we must:

- Preserve and increase the trust and confidence that our citizens, business partners, stakeholders and employees have placed in us;
- Safeguard our information and systems in order to comply with legal and regulatory requirements; and
- Provide clarity, transparency and consistency, in the way we approach our work and how we secure our information.

As a stakeholder, what do I need to do?

All stakeholders need to:

- Evaluate the information and systems for which they are responsible and understand their role in keeping them safe.
- Use good judgment in handling any information with which they are entrusted.
- Understand and apply the appropriate organizational, legal and regulatory requirements in managing highly sensitive or confidential information.

What are the responsilities of owners/ custodians of GORTT information?

The responsibilities are to:

- Handle information in accordance with its sensitivity.
- Maintain your systems in accordance with the applicable information security controls, standards and procedures.
- Be an information security ambassador by promoting awareness and directly influencing behaviour change.

Your checklist

Here is a detailed checklist that you can use to achieve and maintain information security.

Firstly, we need to understand what comprises sensitive information. In the context of TTBizLink, this would include:

Passwords used to access any of the functionalities of TTBizLink

Data maintained on TTBizLink

Documents related to the Cabinet of the GORTT

Defence and security documents

Documents affecting personal privacy

Documents relating to trade secrets

Documents to which secrecy or confidentiality provisions apply

Protecting Information: Treat it Like Cash

To protect your information, please observe the following:

Do not leave keys or key cards used to access confidential information unattended.

Lock your computer with “Ctrl-Alt-Delete” or “Windows-L” when you leave your workstation.

Lock away paper files, laptops, USB drives, external drives, etc. when not in use.

Remove printouts containing confidential information from network printers and securely store away.

Dispose of unwanted confidential information in hard copy by shredding immediately.

Departmental front desk staff should confirm the identity of all visitors entering any restricted areas. IDs should be requested where deemed to be needed. Apply the “need-to-know” principle when allowing access.

Escort visitors to/from meeting area/work areas.

Take note of visitors and report unauthorized personnel to management.

Lock cabinets containing confidential information when not in use.

Lock storage rooms containing confidential information when not in use.

Clear desks, workstations, common work areas, printers and fax machines of all confidential information when not in use.

Refrain from storing confidential information on your personal computer hard drive or external personal devices.

Shut down your computer workstations at the end of the work day.

Do not use your personal e-mail account(s) to share corporate information.

Take particular care when using computer equipment in public places or unprotected areas to avoid being watched or overheard by unauthorized people.

Evaluate your surroundings before discussing sensitive information.

Ensure that confidential information is not left on voice mails.

Unless necessary, avoid removing sensitive documents and data from your office.

Do not conduct meetings in public places.

Remove all information from meeting rooms after the conclusion of the meeting.

Check that the phone line is properly closed after use.

Keeping Passwords Secure!

Particular care is made at TTBizLink to stress the importance of keeping passwords secure as they are the gateway to sensitive personal and company information. Here are some key measures to observe in keeping your password safe:

Passwords should not be written down or stored online.

Do not share any TTBizLink passwords with anyone.

Never use another person's user ID and password.

Do not reveal any password in e-mail, chat, electronic communication, questionnaires or security forms.

Do not speak about a password in front of others.

Always decline the use of the "Remember Password" feature of any application.

All user-chosen passwords should be difficult to guess. Words in a dictionary, derivatives of user-IDs, and common character sequences such as "123456" must not be used. Likewise, personal details such as spouse's name, automobile licence plate, identification number, address and date of birth must not be used. User-chosen passwords must also not be any part of speech. For example, proper names, geographical locations, common acronyms and slangs must not be used.

Do not construct fixed passwords by combining a set of characters that do not change. Additionally, do no choose password that comprise a set of characters that predictably change. In these prohibited passwords, characters which change are typically based on the month, a department, a project or some other easily-guessed factor. For example, if your password is expiring every three (3) months, avoid "X34JAN"; "X34APR"; "X34JUL"; "X34OCT". In this example, "X34" is just added to the abbreviation of the month in which the password is renewed.

Ensure passwords are not the same across different systems such as for your e-mail, bank and social networking accounts.

Create a password that is secure, but still easy for you to remember. To help you remember your password, consider using a phrase or song title as the basis for your password. For example, "Somewhere Over the rainbow" can become Sw0tR8nBo!.

FACT: 76 % of network intrusions exploited weak or stolen credentials.

(2013 Verizon Data Breach Investigations Report)

Beware of Social Engineering and Phishing Attacks

What is a Social Engineering Attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person or researcher and even offer credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's system. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

Social Engineering occurs in many ways and via various channels. Be aware of the following:

Public Places — Public places like cafés, pubs, movie theatres or social networking websites such as Facebook, LinkedIn or Twitter are prime targets for obtaining information. Due to the popularity of social networking sites, care must be taken on what is placed on such sites as it would be visible to numerous persons.

Gossip — In casual and unconstrained conversation, important information might be inadvertently given out.

Personal Pride or Confidence — Sometimes we may give out sensitive information while talking or bragging about ones achievements.

Online — Social engineers may obtain information online by pretending to be the Network Administrator, sending e-mails through the network and asking for a user's password or any sensitive information indirectly. Be very cautious and wary of such requests. We are all too familiar with the lottery schemes where persons receive e-mails indicating that they have won a sum of money but must send certain information to receive the money. This is a popular way of obtaining sensitive personal information.

FACT: 29 % of security breaches leveraged social tactics.

(2013 Verizon Data Breach Investigations Report

What is a Phishing Attack?

Phishing is a form of social engineering, i.e. a fraudulent attempt made through e-mail, phone calls, SMS etc., by seemingly legitimate and trustworthy persons or companies to solicit your personal and confidential information.

Attackers often take advantage of current events and certain times of the year to seek out information, such as:

- *Natural disasters*
- *Epidemics and health scares*
- *Economic concerns*
- *Major political elections*
- *Holidays*

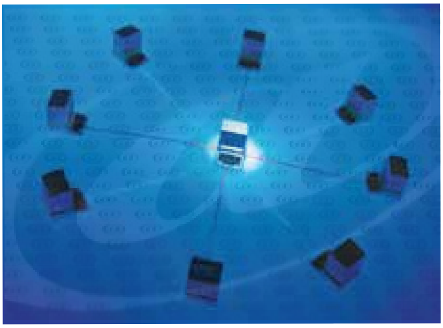
Examples of Phishing Messages: You open an e-mail or text, and see a message like this -

"We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity."

"During our regular verification of accounts, we couldn't verify your information. Please click here to update and verify your information."

“Our records indicate that your account is outdated. You must call us within 7 days to update your account.”

“User #25384: Your profile has been compromised. Text back SENDNOW in order to reactivate your account.”



The senders are phishing for your information so they can use it to commit fraud.

Please note that you will NOT be sent e-mails/text messages or receive any phone calls from TTBizLink or any of its partners requesting your personal information or password.

Any such e-mail, text message or phone call is an attempt to steal your credentials. Never respond to such an e-mail/text message or phone call.

FACT: In 2012-2013, 37.3 million users around the world were subjected to phishing attacks — up 87% from 2011-2012.

(Kaspersky Labs: Evolution of Phishing 2011-2013)

Important Security Tips!

The following are some important tips to note at all times:

The URL address in the address bar of your browser must begin with "https". The letter 's' at the end of "https" stands for 'secured'. Look for https on every page of the TTBizLink website you're on, not just where you sign in.

Do not enter your ttconnect ID or password in any pop up window. Use a pop-up blocker and don't click on any link(s) within pop-ups. If you do, you may install malware on your computer. Close pop-up windows by clicking on the "X" in the title bar.

Only access the TTBizLink website by typing ttbizlink.gov.tt in the address bar of your browser.

Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).

Don't click on any link which has been received via e-mail from an unexpected/untrusted source.

Keep your computer free from malware (short for malicious software that makes you susceptible to computer attacks) and undertake regular scans with Antivirus software to ensure that the system is Virus/Trojan free.

Don't open attachments in e-mails received from unknown senders. Even e-mails that seem to be from friends or family can be a front for malicious activity and lead to malware being installed on your computer.

Update operating system patches regularly.

Avoid accessing TTBizLink from cyber cafés or shared computers.

Be suspicious. Don't get influenced by the unknown person and don't give them any confidential information.

Don't get tempted to use devices which have been left unattended or which you have found.

Don't dump any confidential papers in the trash. Before dumping papers, make sure you don't have any important information in it.

Be cautious. Strangers may try to fool you by creating false situations to solicit personal or confidential information.

Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have that information.

Be suspicious of unsolicited phone calls, visits, or e-mail messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, verify his or her identity directly with the company.

Look at the Secure Sockets Layer (SSL) Certificate details to check the authenticity of the website (click on the padlock symbol in Internet Explorer and/or the site information button in Firefox next to the address bar). Secure socket layer technology protects TTBizLink and allows you to trust the website with your personal information, by encrypting important information during online transactions.

Minimize "drive-by" downloads. Make sure your browser security setting is high enough to detect unauthorized downloads. For Internet Explorer, for example, use the "medium" setting at a minimum.

Resist buying software in response to unexpected pop-up messages or e-mails, especially ads that claim to have scanned your computer and detected malware. That's a tactic scammers use to spread malware.

Download and install software only from websites you know and trust. Downloading free games, file-sharing programmes, and customized toolbars may sound appealing, but free software can come with malware.

Talk about safe computing. Tell your peers that some online actions can put the computer at risk: clicking on pop-ups, downloading "free" games or programmes, opening chain e-mails, or posting personal information.

How do I Detect Malware?

(Malware - short for Malicious Software)

Monitor your computer for unusual behaviour. Your computer may be infected with malware if it:

- *slows down, crashes, or displays repeated error messages*
- *won't shut down or restart*
- *serves up a barrage of pop-ups*
- *displays web pages you didn't intend to visit, or sends e-mails you didn't write*

Other warning signs of malware include:

- *new and unexpected toolbars*
- *new and unexpected icons in your shortcuts or on your desktop*
- *a sudden or repeated change in your computer's internet home page*
- *a laptop battery that drains more quickly than it should*

What do you do if you think you are a victim?

If you know or suspect that access to your information has been compromised you should immediately:

- Change your password
- Update your security software then run a full scan on your computer for malware
- Report your security incident to your internal IT and the TTBizLink Help Desk by calling **800-4SEW/4739**, weekdays from 8:00 a.m. to 4:00 p.m. or send an e-mail to **support.ttbizlink@gov.tt**

For further information view our videos and test your knowledge on information security by taking our quizzes. It's on the "Our Security Alert" webpage that you will encounter during the login process. We also encourage you to contact us if you need further explanation on any information in this brochure. See contact number and e-mail above.

INFORMATION SECURITY IS
EVERYONE'S RESPONSIBILITY