DGSI
RECRUITMENT & WORKFORCE SOLUTIONS

Design Group Staffing

INTEQNA

talentcor

IT Security Best Practices

DGSI END-USER PC BEST PRACTICES

Web Browsing

Limit Web browsing to work-related sites

Be vigilant of downloading software or files from the Internet. Visiting sites not intended for DGSI work purposes can result in unwanted web content being delivered to our desktops. Web sites and end users clicking on targeted links are the #1 entry point of malicious software into corporate networks.

How can I be sure that a website is genuine?

Some web links, especially ones that are a part of phishing schemes, will redirect to fraudulent web pages; even when entering Internet addresses into your browser by hand, you might end up at a phisher's site if the address you enter is non-secure or incomplete, or is automatically completed or redirected by your browser.

Unfortunately, when you access non-secure websites (i.e., those sites whose addresses use an http:// prefix), you can do nothing to verify that you have not been redirected to a fraudulent site. However, when accessing secure sites, including most commercial, financial, and university services, you can protect yourself by making sure that the site you are visiting is the page you want to get to. To do this, type the entire URL, including the initial https://, into your browser.

Virus Alerts

Don't click on popup windows that tell you that your computer is infected with a virus:

Antivirus software doesn't work that way. Those popups install malware onto your computer, with your permission. Sometimes it's a scam that requires you to pay money to have the software removed by the software originator. Don't fall for it. Contact DGSI helpdesk immediately if you see any message stating this.

How can I tell if a computer virus alert is a hoax?

Two key factors make a successful virus hoax: (1) technical-sounding language and (2) credibility by association. If the warning uses the proper technical jargon, even the technologically savvy can be fooled. Nevertheless, if a virus alert you receive contains technical-sounding language and comes from a seemingly authoritative source, it may also be a true virus alert.

Do not download unfamiliar software off the Internet

Some programs will appear to have useful and legitimate functions. However, most of this software is (or contains) spyware, which will damage your operating system installation, waste resources, generate pop-up ads, and report your personal information back to the company that provides the software.

Do not click random links

Do not click any link that you can't verify. To avoid virus spread via email or instant messaging (IM), think before you click; if you receive a message out of the blue, with nothing more than a link and/or general text, do not click it. If you doubt its validity, ask for more information from the sender, or contact the DGSI helpdesk and they will assist you in identifying the risk associated with the link.

Password Management

We all have too many passwords to manage - and it's easy to take short-cuts, like reusing the same password.

Here are some general password tips to keep in mind:

- Use long passwords - **20 characters or more is recommended.**
- Use a strong mix of characters, and never use the same password for multiple sites.
- Don't share your passwords and don't write them down (especially not on a post-it note attached to your monitor).
- Update your passwords periodically, at least once every 6 months (90 days is better). On the DGSI Network, you will be forced to change your password every 90 days.

E-mail Management

In general, do not open unsolicited or unrecognized e-mail. Do not send confidential or sensitive information without proper authorization.

Fraud and misrepresentation

Dishonest users sometimes attempt to forge mail messages to others to gain personal information, such as account passwords or even credit card information. Do not ever divulge such personal data in a reply, even if the sender looks legitimate; instead, forward the suspicious mail to DGSI Helpdesk for further scrutiny.

Avoiding spam

Spam has increasingly become a problem at DGSI. While every user receives some spam, email addresses posted to websites or in newsgroups and chat rooms attract the most spam.

To reduce the amount of spam you receive:

- Filter your email: Your email client or web-based email provider may have other methods for setting up email filtering. Many offer blacklisting, which prohibits mail sent from email addresses that you list. Even more restrictive is whitelisting, which blocks mail sent from anyone except those that are on the list.
- Don't reply to spam under any circumstance.
- Do not use your corporate DGSI email address to any website for login, notification or subscription purposes.

Be careful releasing your email address, and know how it will be used

Every time you communicate on the Internet or browse a website, there are opportunities for spammers to intercept your communications to obtain your email address and other personal information. Otherwise reputable companies may sell or exchange your email address with other companies, and this information may eventually find its way to a spammer. Consider the following guidelines:

- Subscribe only to essential discussion lists, and ensure that they are moderated.
- Think twice before offering your email address to a website. Check the DGSI privacy policy for that guidelines on offering corporate information onto public web sites. The policy can be found here: http://security.dgsi.ca/ITSecurity&Privacy.pdf

Be careful with email attachments

Beware of email or attachments from unknown people, or with a strange subject line: Never open an attachment you weren't expecting, and if you do not know the sender of an attachment, delete the message without reading it. If it's from someone you don't know, delete the email or identify it as spam. To open an attachment, first save it to your computer and then scan it with your antivirus software; check the DGSI help desk for instructions.

FOR YOUR HOME NETWORKS

Always use a device firewall

A personal or operating system firewall is an excellent line of defense against malicious software that attempts to connect out to its home server. You'll receive a warning when an attempt is made, and you can optionally block the communication. Blocking the communication won't remove the infection, but it will render it mostly harmless, especially if it is one of the many "logger" infections that grabs your data as you type it into websites or client software.

Keep your operating systems and software up to date

Yes, it's a pain to update your apps and operating systems up to date because doing so often requires a reboot. Your device will react slowly while the device updates, but it's for your own good. Take a tea break, watch an old episode of The IT Crowd or take a walk until your updates have finished.

Never download pirated or cracked software

This type of software almost always includes some type of malware. Plus, it's illegal to steal software, so there's that aspect of it. If you're using a corporate computer and you download pirated software onto it, you're jeopardizing your job because your company can get into big trouble for harboring pirated software.

Public Wi-Fi

Limit what you do over public Wi-Fi and apply the following best practices when using it:

- It’s best not to use a public Wi-Fi network without VPN. Rather use your cell network when security is important (3G/4G/LTE).
- When using public Wi-Fi ask the vendor for the correct name of the Wi-Fi Access point and confirm that it has security. It is common for hackers to publish their own Wi-Fi SID with similar names.
- Disable Auto Connect Wi-Fi or enable Ask to Join Networks. Hackers use Wi-Fi access points with common names like ‘Airport’ or ‘Café’ so your device will auto-connect without your knowledge. Never opt to remember the Wi-Fi network on public access points.
- Use the latest web browsers as they have improved security for fake websites. This prevents someone from hosting their own ‘Facebook’ website, for example, waiting for you to enter your credentials.
- Do not click on suspicious links like videos, even via social chat.
- Beware of advertisements. They could direct you to compromised websites.
- Use a least privileged user or standard user while browsing as this will significantly reduce the possibility of malicious malware being installed.
- Always assume someone is monitoring your data over public Wi-Fi.
- Do not access your sensitive data like financial information over public Wi-Fi.
- Do not change your passwords, and be wary of entering any personal credentials while using public Wi-Fi.
- If you have a mobile device with a personal hotspot function, choose this over public Wi-Fi where possible—but still be cautious.