Top 10 Cyber Security Tips

For NSW Government Employees – Case Studies

Choose unique passwords only

Use it for just one account. Think of a long phrase or a story that is unique to you but impossible for someone else to know and consider using a reputable password manager for any personal accounts.

Why does this matter?

Reusing the same password puts both you and your organisation at a much greater risk of potentially catastrophic consequences.

In 2012 a Dropbox employee reused their LinkedIn password on a corporate system resulting in a data breach that effected 60% of Dropbox users.

Be wary – Phishing emails are designed to look legitimate

Stop and think before you click on links or open attachments. Always check if you know who the email is from and never give out personal information such as credit card details, bank account details or passwords.

Why does this matter?

Scammers often make their emails more convincing by performing reconnaissance against the intended victim first. More and more, everyday citizens are being fleeced out of their life savings due to poor cyber security which is exploited by financial scammers.

Never leave your devices unattended

If you are stepping away from your desk, lock your screen with a unique password.

Why does this matter?

Compromise of national security is not a phrase you ever want to hear, especially if you are a special agent in the United States Secret Service. But this is exactly what happened after a laptop containing highly sensitive information was stolen out of a secret service agent's car.

Thieves like easy targets. Protect yourself by always locking your computer when leaving your desk, storing your computer in a secure manner and never leaving your computer unattended in an unsecure environment.

A quick way to lock your computer is to use the Windows Key + L.

Keep your operating systems up to date

Configure automatic updates on all devices to ensure that systems remain secure.

Why does this matter?

Updates often fix vulnerabilities that attackers can find and use to access your system. It's an effective way to help keep them out. In 2017 the WannaCry attack affected thousands of computers worldwide and brought mission critical infrastructure across a wide range of sectors including finance, medical, and transport to a halt. If the victims had upgraded their systems to Windows 10 they wouldn't have been affected.

Set up multi-factor authentication (MFA) on your devices

An additional form of authentication should be placed on all accounts where possible.

Entering a username and password combination does not provide sufficient security against online threats. There are numerous options for doing this which include: authenticator apps, biometrics, smart cards, hardware security tokens or one-time pins sent to another device online. This is an added layer of security which helps stop attackers getting into your accounts.

Why does this matter?

In a world where credential harvesting is a constant threat and over 80% of hacking-related breaches are caused by stolen or weak passwords. MFA helps reduce the risks of compromised passwords. It adds another layer of protection from the kinds of damaging attacks that cost organisations millions.

For more information, please contact Cyber Security NSW via community@cyber.nsw.gov.au

Top 10 Cyber Security Tips

for NSW Government Employees – Case Studies

Limit the use of your work email address for personal use

Use a personal email address for all non-work related matters

Why does this matter?

Using a work email address for personal use increases the chances of being targeted in Phishing campaigns. If a company that possesses your email address is compromised, your email address may then be added to mailing lists used by cyber criminals. For example in Germany, more than four years after the 2012 LinkedIn breach, German corporate executives were still being targeted with malicious emails from hackers who had obtained the leaked contact details. The ongoing spear-phishing attempts were shown to be consistent with credentials leaked in the 2012 LinkedIn breach.

Try not to use free Wi-Fi or internet hot spots

When connecting to public Wi-Fi, use a reputable virtual private network (VPN). If connecting to an organisation's Wi-Fi, ask an employee to point out the correct SSID (network name) and the password to ensure you are not connecting to an attacker's hotspot.

Why does this matter?

One of the biggest threats with public Wi-Fi is the ability for hackers to position themselves between you and the connection point. So, instead of talking directly with the hotspot, you end up sending your information to the hacker. The hacker also has access to every piece of information you send out. In 2014 a sophisticated hacking campaign called "Dark Hotel" was discovered which targeted CEOs, government agencies, U.S. executives, NGOs. When executives connected to their luxury hotel's Wi-Fi network and downloaded what they believed were regular software updates, their devices were infected with malware. Today's Public Wi-Fi standards are flawed and should not be trusted. You could be connecting to an insecure network or poorly protected network which could be easily accessed by other parties.

Stay smart with social media

Be wary of posting information you wouldn't want a stranger to know. What you post on social media can give cyber criminals information that they can use against you. Set your privacy so only friends and family can see your details.

Why does this matter?

Information that people post "can be used to craft a targeted phishing email containing a malicious link," which raises the probability that people will take the bait. Hackers often target victims who they know are on holiday overseas or during holiday periods at work. This is true both in CEO fraud scams where the hacker impersonates a CEO seeking payments, or grandparent scamming where the hacker pretends to be an injured relative on vacation needing money urgently.

Check bank statements regularly

Keep an eye on work and personal bank statements and bank account numbers to check you know the source of the transaction and consider applying for a free annual credit report from a credit reporting agency.

Why does this matter?

In 2014, US authorities noticed several "Free Domino's Pizza" groups being run on Facebook. Whilst seemingly innocent, it turned out to be a front for a large criminal operation testing stolen credit card information. The criminals would order pizza to confirm the card was valid and then send the delivery to random Facebook users so not to be linked to the order themselves. By regularly monitoring bank statements and accounts, users can quickly identify unknown purchases and follow up with their bank provider. This can help alert security teams of possible security breaches early on and prevent more disastrous outcomes.

Familiarise yourself with your organisation's acceptable use policy or speak to your local IT Security contact

If you see something of concern, report it immediately to your IT Security team.

Why does this matter?

In February 2019, Bunnings Warehouse experienced a privacy breach by one of its own employees. The staff member had created a database to distribute emails about upcoming events at the store he worked at, and in doing so, he exposed private staff and customer information that included employee performance reviews, login credentials, physical and email addresses, and phone numbers. While unlikely that the staff member had intentionally leaked the database content, his creation of the database itself constituted a breach of Bunnings' data policy guidelines.

The employee probably thought he was doing Bunnings a favor, but he really should have been clear on the company's acceptable use policy!

For more information, please contact Cyber Security NSW via community@cyber.nsw.gov.au