‘It won’t happen to me’ ...
Can you be certain of that?

Knowing how to prevent and respond to social engineering can protect you and your workplace.

**What you can do:**
- Ensure you understand the value of the information you hold. It may seem arbitrary in isolation, but pieces of information drawn from different sources can allow someone to form a picture of your identity or your organisation’s security.
- If you receive a suspicious phone call or email, note down as much detail as you can about the incident:
  - What kind of information was the person trying to obtain?
  - What area of your organisation was targeted?
  - Where were you targeted, for example at home, at work or travelling for business?
  - Is this just one incident or is there a pattern/frequency?
  - What damage has been caused?
- Report suspicious emails to your ICT Service Desk.
- Report other suspicious contacts to your Agency Security Advisor or other Security Personnel.

**Need more help?**
- Read your organisation’s security policies.
- www.staysmartonline.gov.au has information about how to protect yourself and your family from social engineering.
Introduction

As technology becomes more sophisticated and organisations more prepared for external attacks, social engineering has emerged as a low cost - high value tool for people wanting to steal your information.

Social engineering requires very little technology, instead relying on the exploitation of trust, human relations and publicly available information.

As more people commit to social media as a way of living and socialising, our information and privacy becomes more vulnerable.

Understanding the connection between your professional and personal information is critical to keeping your information safe.

What is social engineering?

Social engineering is an attempt to obtain your passwords or personal details by tricking you into giving up your confidential information.

Unlike computer-based hacking, you may be targeted via phone calls, email or even in person. Often an attacker will do research on an organisation before making contact, so it will appear as if they know things that only a colleague would know.

This builds trust and can result in the victim giving up valuable information all the while believing the person is a fellow employee.

The person may have used mapping software to get a visual of your office and nearby cafes that are frequented, or used social media like LinkedIn to build a profile of job roles, hierarchy and operating systems at your organisation.

They may target many different people simultaneously so that in isolation their questions appear unimportant. It is when this information is pieced together that someone who seeks to do harm can form a picture of how best to target you or your organisation.

How secure is your information?

Our society is now experiencing a hyper-information age. As an individual, the choices you make every day in relation to your information can have a great impact on your safety and your privacy.

Some things to think about:

- It’s not just corporate information criminals are after, it’s your personal details too. If enough of your personal information is available in public, or you give this to someone who deceives you, they may be able to access your bank accounts and impersonate you.
- Ensure your privacy settings are switched to high for all social media - work or personal - and check this regularly.
- Only accept social media requests from people you know and trust.
- Avoid uploading your CV or including details on your profiles that could reveal security information about your work or home.
- Ensure you change your passwords regularly, and choose passwords that are difficult to guess.

Potential ‘red flags’

Be cautious of:

- Emails and phone calls from people asking questions about your finances or computer, employees, or security procedures.
- External third-party software/USBs given as gifts - always have these checked with your ICT Service Desk before use.
- Phishing - emails that appear to originate from a trusted and legitimate source, like your bank or a fellow employee. These often contain hidden links (shown when hovering), spelling errors and unexpected attachments. Never give out your username and password to anyone.

How to spot a phishing email

From: Neighbourhood Bank Security Team
<NeighbourhoodBank331.com.au>
Reply-To: <000000000@0000.com>
Subject: [SPAM] We suspect Your Account has been Accessed

This message has been automatically generated due to suspected illegitimate activity on your account. We are currently investigating this issue, and will be in contact when it is resolved. Please validate your details below to avoid this happening in future:

Name:
Address:
DOB:
Neighbourhood Bank Account No:
Online Password:
Confirm Password:

Commands and threats:
Failure to validate your Account may result in continued illegitimate activity. Please keep yourself safe with our help.
Thank you for your cooperation.

Neighbourhood Bank Security Team
No contact information
Introduction

As technology becomes more sophisticated and organisations more prepared for external attacks, social engineering has emerged as a low cost - high value tool for people wanting to steal your information.

Social engineering requires very little technology, instead relying on the exploitation of trust, human relations and publicly available information.

As more people commit to social media as a way of living and socialising, our information and privacy becomes more vulnerable.

Understanding the connection between your professional and personal information is critical to keeping your information safe.

What is social engineering?

Social engineering is an attempt to obtain your passwords or personal details by tripping you into giving up your confidential information.

Unlike computer-based hacking, you may be targeted via phone calls, email or even in person. Often an attacker will do research on an organisation before making contact, so it will appear as if they know things that only a colleague would know.

This builds trust and can result in the victim giving up valuable information all the while believing the person is a fellow employee.

The person may have used mapping software to get a visual of your office and nearby cafes that are frequented, or used social media like LinkedIn to build a profile of job roles, hierarchy and operating systems at your organisation.

How secure is your information?

Our society is now experiencing a hyper-information age. As an individual, the choices you make every day in relation to your information can have a great impact on your safety and your privacy.

Some things to think about:

• It’s not just corporate information criminals are after, it’s your personal details too. If enough of your personal information is available in public, or you give this to someone who deceives you, they may be able to access your bank accounts and impersonate you.

• Ensure your privacy settings are switched to high for all social media - work or personal - and check this regularly.

• Only accept social media requests from people you know and trust.

• Avoid uploading your CV or including details on your profiles that could reveal security information about your work or home.

• Ensure you change your passwords regularly, and choose passwords that are difficult to guess.

Potential ‘red flags’

Be cautious of:

• Emails and phone calls from people asking questions about your finances or computer, employees, or security procedures.

• External third-party software/USBs given as gifts - always have these checked with your ICT Service Desk before use.

• Phishing - emails that appear to originate from a trusted and legitimate source, like your bank or a fellow employee. These often contain hidden links (shown when hovering), spelling errors and unexpected attachments. Never give out your username and password to anyone.

How to spot a phishing email

This message has been automatically generated due to suspected illegitimate activity on your account. We are currently investigating this issue, and will be in contact when it is resolved. Please validate your details below to avoid this happening in future:

From: [Neighbourhood Bank Security Team <NRT1@neighbourhoodBank@AUS.COM.AU>]
Reply-To: [000NRT1@neighbourhoodBank@AUS.COM.AU]
Subject: [SPAM] We suspect your account has been accessed.

Dear [name],

This message has been automatically generated due to suspected illegitimate activity on your account. We are currently investigating this issue, and will be in contact when it is resolved. Please validate your details below to avoid this happening in future:

Name:
Address:
DOB:
Neighbourhood Bank Account No:
Online Password:
Confirm Password:

Commands and threats:
Failure to validate your account may result in unintended activity. Please keep yourself safe with our help.

Thank you for your cooperation.

Neighbourhood Bank Security Team

[Contact information]
Knowing how to prevent and respond to social engineering can protect you and your workplace.

What you can do:
• Ensure you understand the value of the information you hold. It may seem arbitrary in isolation, but pieces of information drawn from different sources can allow someone to form a picture of your identity or your organisation’s security.
• If you receive a suspicious phone call or email, note down as much detail as you can about the incident:
  ◦ What kind of information was the person trying to obtain?
  ◦ What area of your organisation was targeted?
  ◦ Where were you targeted, for example at home, at work or travelling for business?
  ◦ Is this just one incident or is there a pattern/frequency?
  ◦ What damage has been caused?
• Report suspicious emails to your ICT Service Desk.
• Report other suspicious contacts to your Agency Security Advisor or other Security Personnel.

Need more help?
• Read your organisation’s security policies.
• www.staysmartonline.gov.au has information about how to protect yourself and your family from social engineering.