Cyber Security Briefing

Passwords – Email – Internet – Phone – Social Media

Passwords

1. The most common method of any illegal access to an account is by having an insecure password protecting your account. So what is an insecure password?

- **Sequential/Keyboard Patterns:** 123456, 111111, qwerty, asdfgh
- **Simple Words:** password, login, welcome, iloveyou
- **Username/Service Based:** admin, password, or variations of the service name (e.g. Target12345)
- **Short/Simple Alphanumeric: 12345678, 1234567890**
- **Weak Combinations:** Aa123456, p@ssw0rd
- **Names/Pop Culture:** superman, princess, dragon, harrypotter

2. **Why these are insecure:** These passwords are at the top of hacker dictionaries and can be cracked in less than a second using automated, “brute-force” attacks. Using these passwords ensures your accounts are highly vulnerable to unauthorised access.

3. **Once your password is compromised** it can be used to access personal emails/details which will enable the someone to create a duplicate identity using your credentials which can then be used to take loans etc in your name.

Email Security

1. One of the common methods of installing malicious code/programs onto your desktop/laptop/tablet/phone allowing unauthorised access is for an email recipient to click on a link contained in an email.

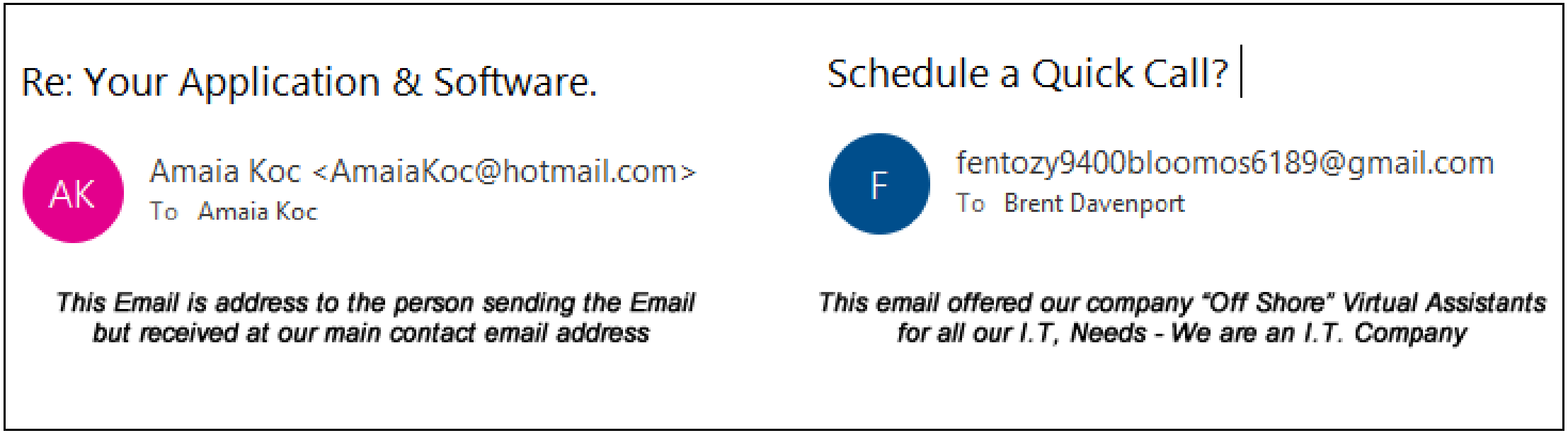
The Golden Rule

“You Get Nothing for Nothing”

2. Beware of any free or special offers received by email

Email Security

3. Beware of any commercial approach from an organisation offering any service when using a free email address.



4. In both instances the email examples above were received from email addresses created free of charge from hotmail.com & gmail.com.

Email Security

5. If you consider the low-cost price or registering a website name (domain name), creating a website and a company email there is no reason whatsoever for a person or genuine company offering goods and services to use any form of free email addresses from hotmail, outlook, google, yahoo etc, so send this type of email to your junk folder and forget about it.

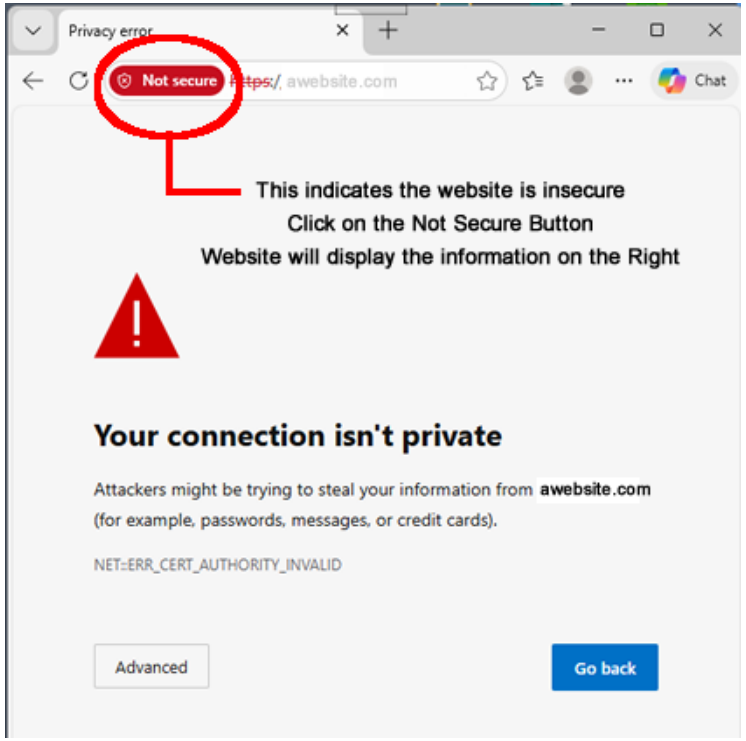
The only reason why senders of this type of email do not register a genuine domain name is that full contact details have to be provided to complete a registration. These senders have no interest in advertising who they are or where they are located.

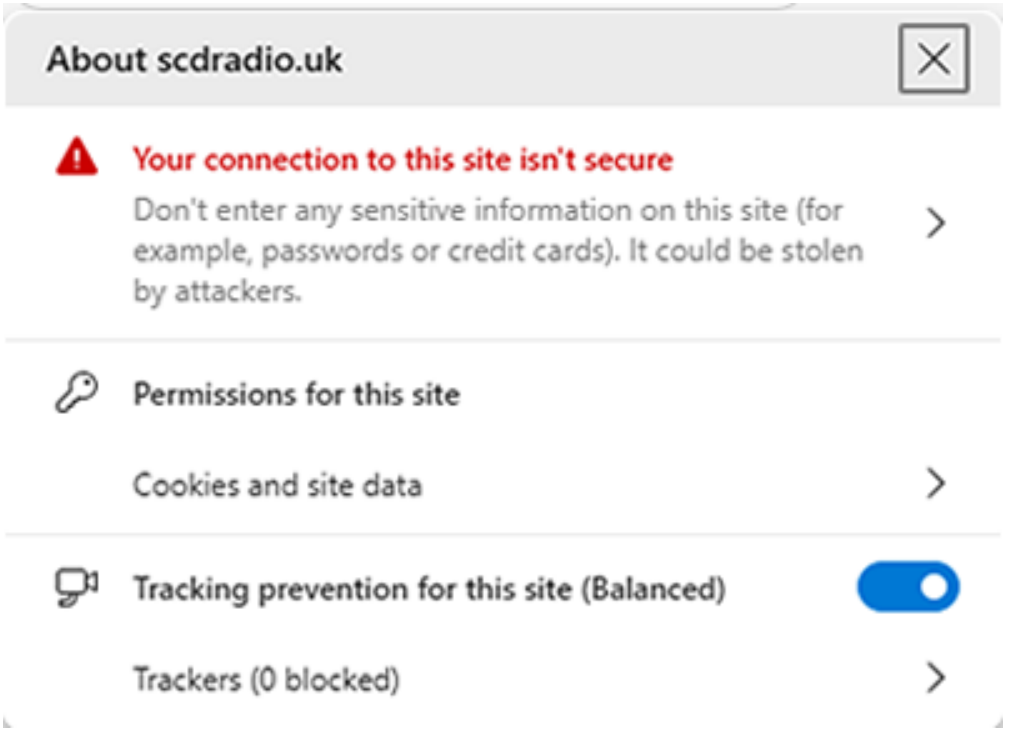
6. **You may ask "why do I receive these emails"?** The answer is phishing emails are sent to get a response, which will confirm your email address is genuine or give attackers the ability to install scripts on your machine to gain the necessary information discussed during the Password section of this presentation.

7. Further, never answer, reply to or click on any link contained in an email from such a source as this action confirms they have reached a genuine email, which could result in further issues.

Website Security

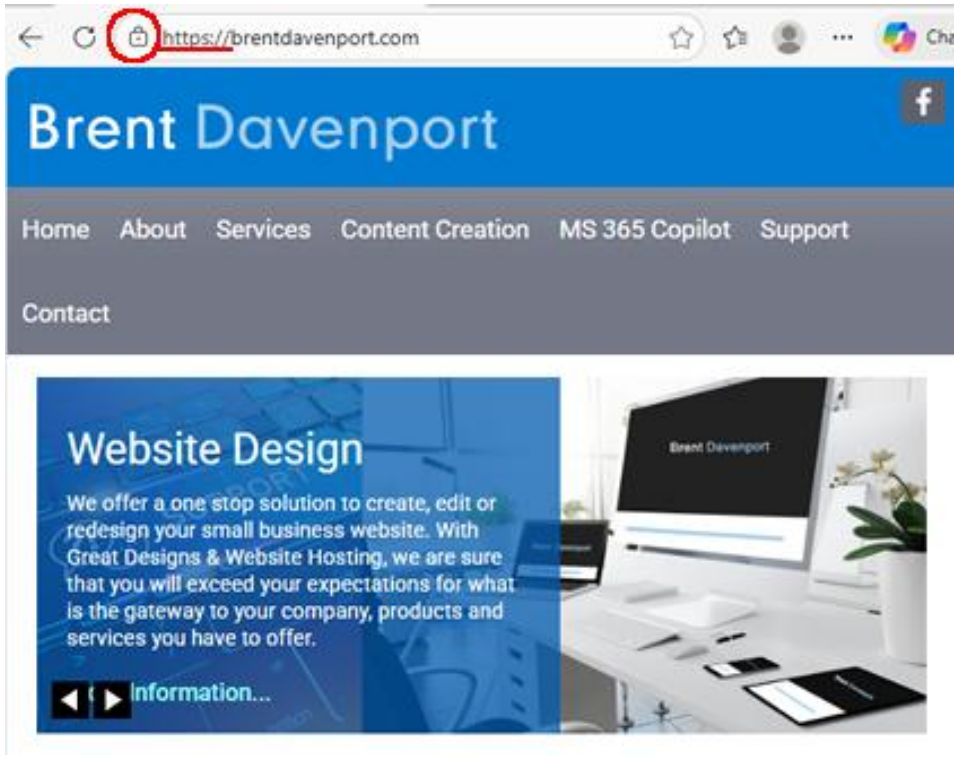
1. When you visit an insecure website your web browser will display the following:-



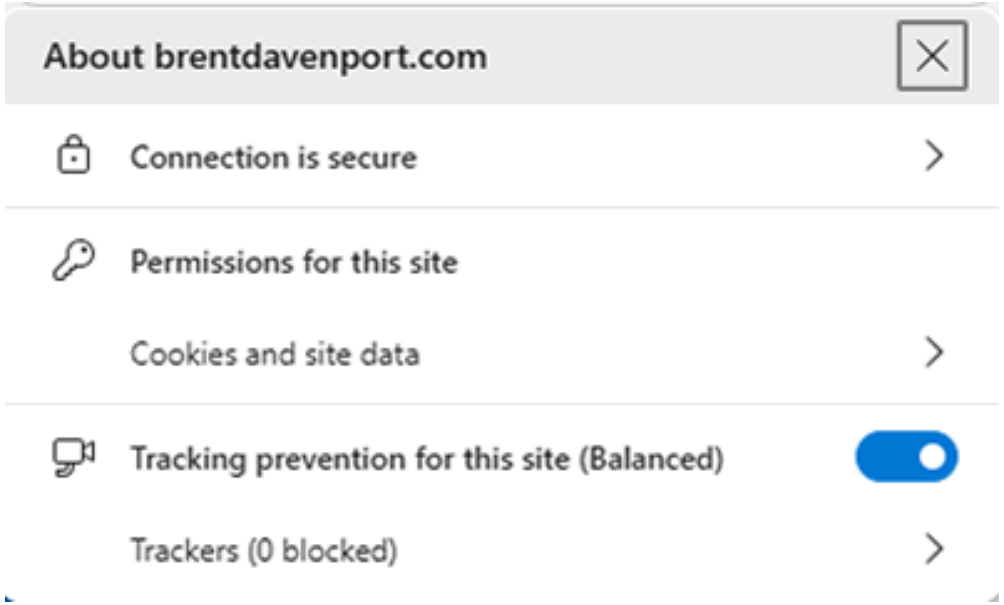


Website Security

2. A genuine (secure) website will have a padlock symbol (this may vary from browser to browser but always top left before the website URL) also to indicate the website is safe the first part of the website address will always begin with HTTPS:// as underlined in the image below with the red line.



3. When you click on the padlock symbol you will be able to view the information below:-



Mobile Phone Security

1. Any form of cold call on your phone should always be suspected. You will never receive calls from your bank or credit card company, should you receive such a call immediately close the call down and call your bank/credit card company directly. Never allow anyone you do not know to install any kind of software on any of your devices, in particular Any Desk.

2. Recently the "**Mum & Dad" mobile phone scam** has been identified by cyber security advisors. This scam is a type of impersonation fraud where scammers send a text message pretending to be a child who has lost or damaged their phone. They then convince the parent to continue the conversation on a new phone number before eventually requesting money. This emotional tactic leverages urgency and trust to convince parents they are helping a loved on, when in fact they are communicating with criminals

Social Media & Instant Messaging Security

1. Social media presents a significant challenge in respect of personal security. We often share personal information that could be exploited by cyber criminals for identity theft or phishing attacks. We have recently seen an increase in fake accounts trying to contact our company.

   As an example, I recently received a contact from an old friend from my military days, the conversation started out of the blue with “Hi how are you”? After a couple of replies I realised this was a suspicious contact, I confirmed my suspicions with a simple question “Where did we meet”? The contact immediately disappeared.

2. To stay safe, you should limit what you share by using strong privacy settings and remain cautious of unsolicited messages or suspicious links.

Finally

1. The subject of cyber security is large and complex. You should understand that the primary protection is delivered by yourselves providing you follow the simple rules outlined during this presentation.

- **Passwords** – We introduced 8 letter/number/capitals/symbol password in 2012 for our clients, since we introduced this policy, we have not had one report of any security access incidents. We are currently updating our clients' password to 12 characters.

- **Multifactor Authentication** – This is used by most banks and organisations. Take advantage of this facility when offered as it will give you an extra level of protection.

2. In today's modern world the use of online facilities is necessary in our daily lives, don't let it frighten you, just use these facilities in a safe manner.

Thank You For Your Time

Any Questions?