Scams, Fraud and Other Dangers

7 Additional Security Matters

- Scams and fraud
- Cybersecurity
- Data leaks
- Encryption – symmetric, asymmetric, public key
- Loyalty cards
- Passwords – how are they stored on the servers?
- Social media – Facebook, Linkedin

7.1 Scams and Fraud

- Record losses -- >$500 million (Australia) by end of 2019 (ACCC)
- Phishing,
- Identity theft
- Fraud
- Business Email Compromise (BEC)
- Deepfake
- Ransomware
- Sextortion

7.2 Phishing

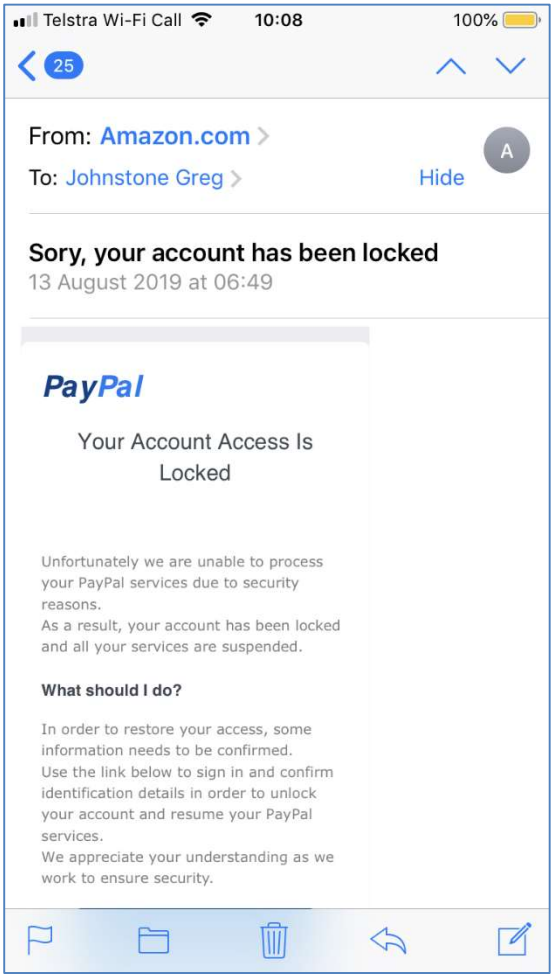
Phishing is a cybercrime in which a target is contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords.

7.2.1 Protect yourself

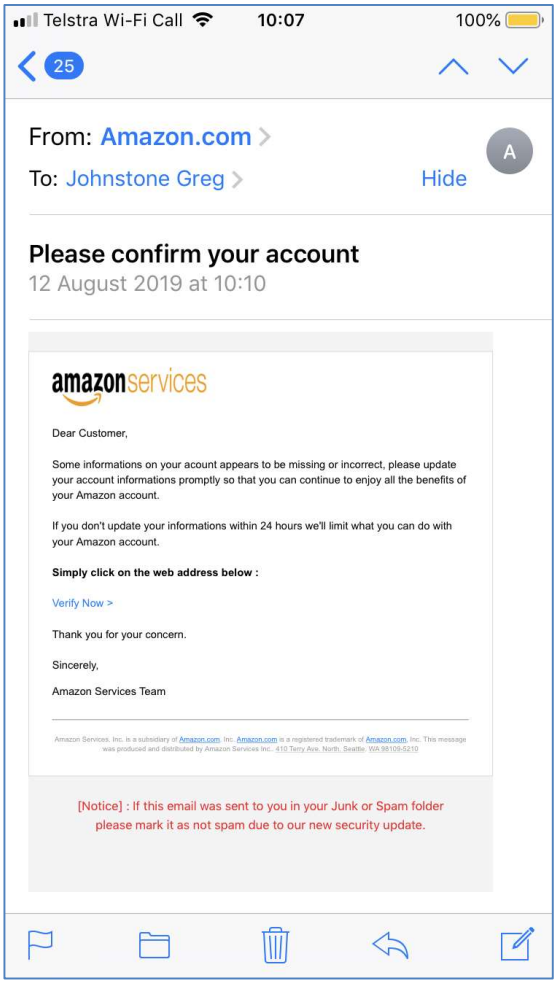
Beware of unexpected emails, messages or calls from organisations that you have a financial relationship with – ATO, your bank, Netflix …

- Learn to recognise the signs:
    - Poor grammar
    - Not addressed to you (e.g. Dear customer)
    - May use threatening language
    - Asks you to verify your details or click on a link
    - Usually expresses urgency
- Use a password manager
- Use a good (paid for) anti-virus
- Use 2-factor authentication (2FA)
- Check links before clicking on them (sometimes difficult to do -- find out how to do it on your device)
- Check the sender – practise with a good email

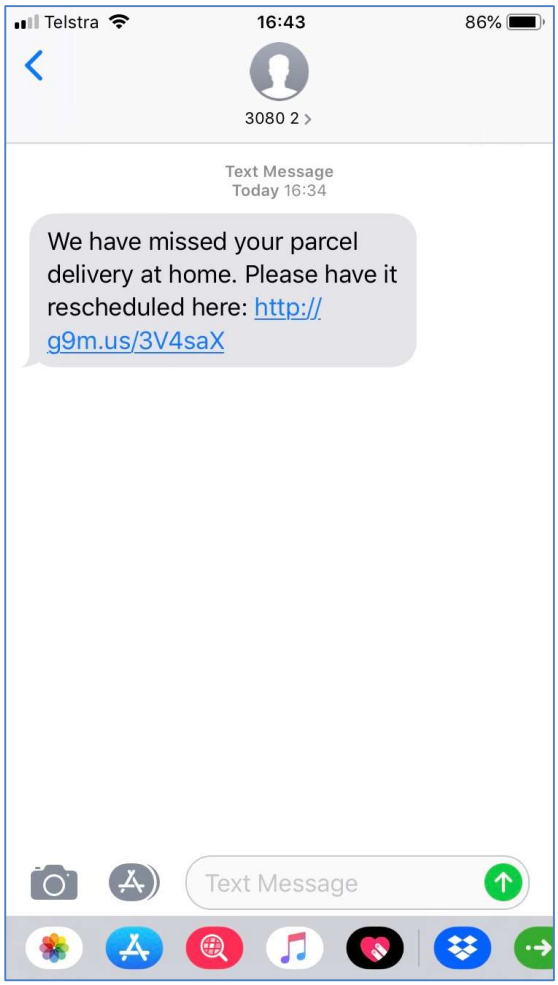
Examples:



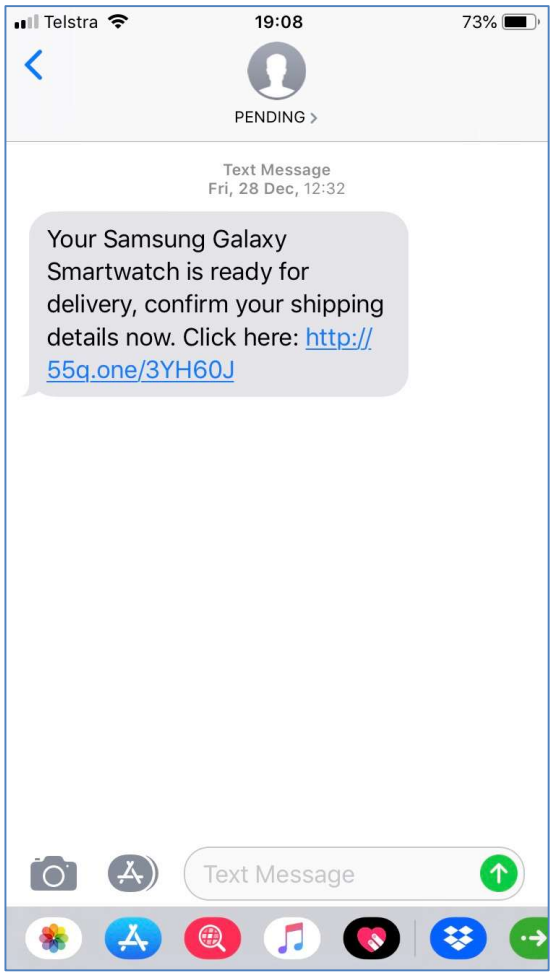
Poor grammar, spelling errors



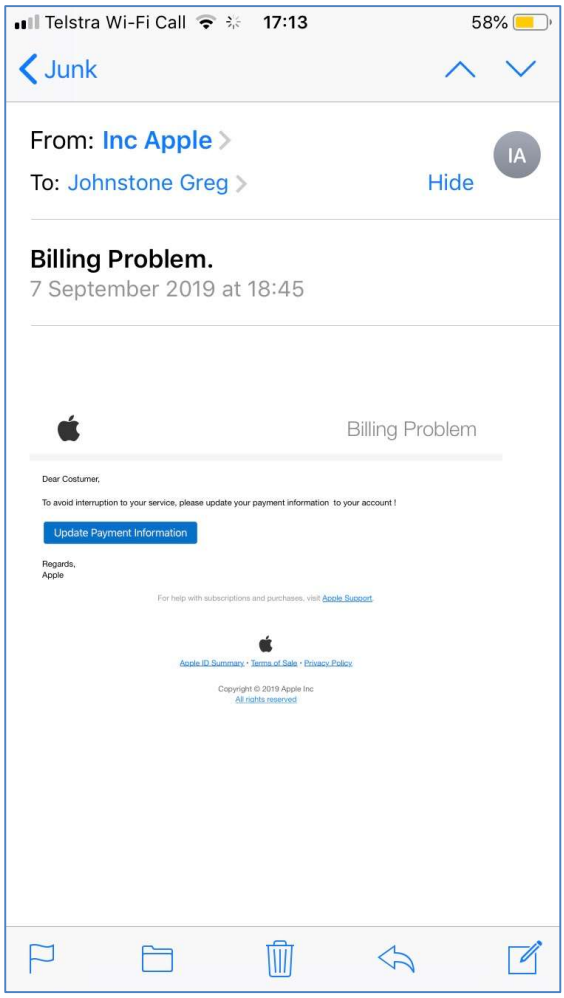
Asks to confirm your account (no-one ever does that)



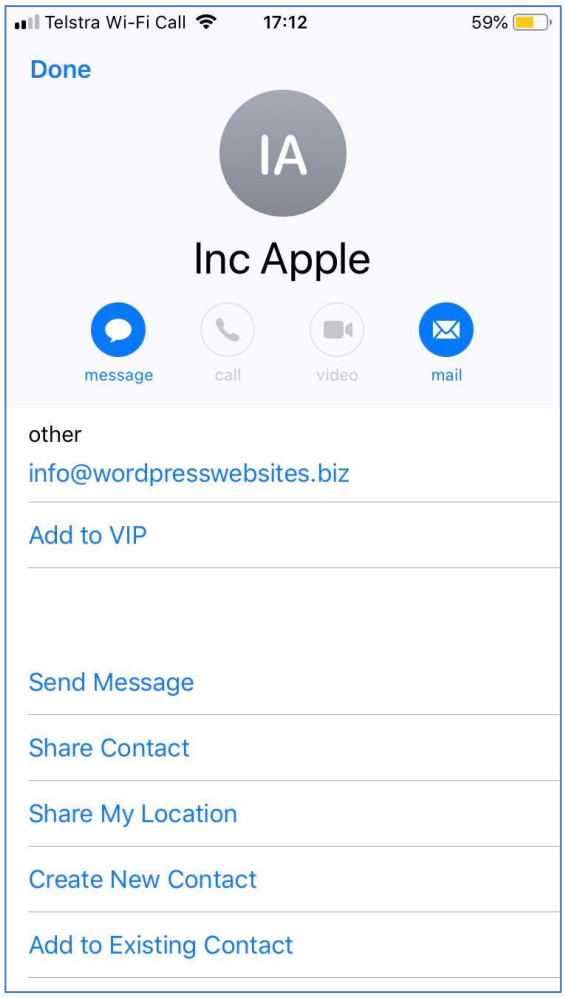
I didn't order anything



I didn't order this



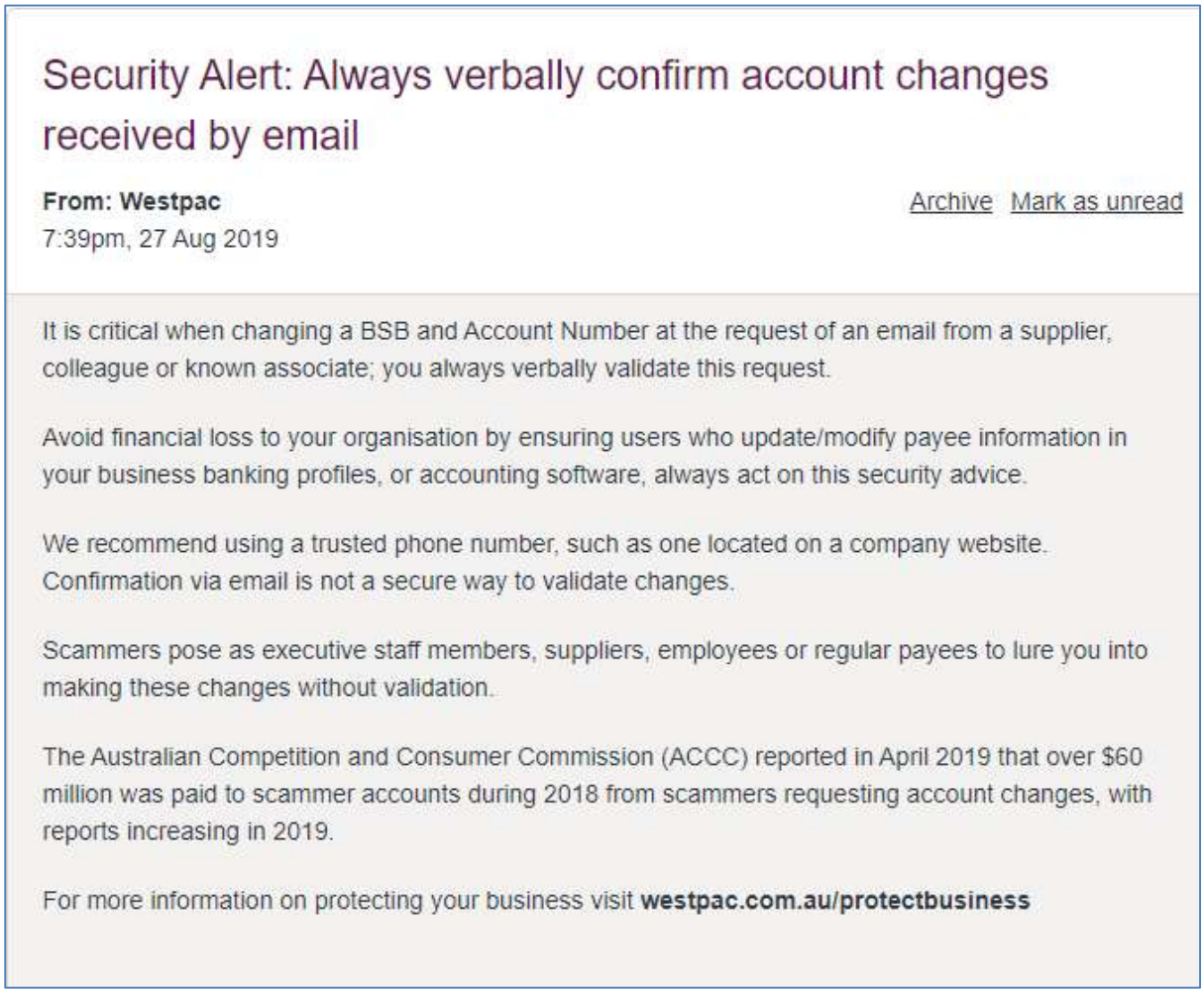
Check the sender (press and hold From address), not an Apple domain.



This is not from Apple

7.3 Business Email Compromise (BEC)

It's not just businesses that fall foul of this of this scam. Banks do not confirm that BSB and Account Number matches Account Name, leading to possible fraud:



Security Alert: Always verbally confirm account changes received by email

From: Westpac
7:39pm, 27 Aug 2019

Archive Mark as unread

It is critical when changing a BSB and Account Number at the request of an email from a supplier, colleague or known associate; you always verbally validate this request.

Avoid financial loss to your organisation by ensuring users who update/modify payee information in your business banking profiles, or accounting software, always act on this security advice.

We recommend using a trusted phone number, such as one located on a company website. Confirmation via email is not a secure way to validate changes.

Scammers pose as executive staff members, suppliers, employees or regular payees to lure you into making these changes without validation.

The Australian Competition and Consumer Commission (ACCC) reported in April 2019 that over $60 million was paid to scammer accounts during 2018 from scammers requesting account changes, with reports increasing in 2019.

For more information on protecting your business visit **westpac.com.au/protectbusiness**

7.4 Dangers

- Any program (executable, macro, script)
- Data leaks
- DDoS
  Distributed Denial of Service. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a Trojan, are used to target a single system causing a Denial of Service (DoS) attack.
- Do not post your email address or phone number online (eg on a blog or social media site)
- Email masquerade (emails pretending to come from someone else, usually someone you know).
- Exploits
- Extortion – online dating, ransomware, hitman – Ebola scam
- Fake extensions (Microsoft)

- Fake invoices
- Fake links
- Flash (Adobe)
- Free USB sticks
  Free USB sticks often contain malware – some can contain software that wipes your computer.
- Hacking
- Human error (NAB emailed account details to nab.com instead of nab.com.au)
- Identity theft
- Infected email – email attachments (payloads)
- Infected websites – ransomware often originates from infected web sites. A good quality anti-virus should warn you if the site you want to visit is infected.
- Key fobs (garage door, intruder alarm)
- Key loggers – a device or software (malware) that logs every keystroke, usually for the purpose of stealing passwords.
- Microsoft Word and Excel macros
- Proxy Server – A proxy server is a computer system or router that functions as a relay between client and server. It helps prevent an attacker from invading a private network and is one of several tools used to build a firewall.
- Public Wi-Fi – do not use under any circumstances
- Scams – Phishing, Nigerian, phone calls (I'm from Microsoft and we've noticed a virus on your computer – Really?). I'm from the tax office and we're laying criminal charges against you. Also, people claiming to be from Centrelink.
  - Invoice substitution scam – resulting from a hacked email account.
  - 'Sharing websites' – Uber, Airbnb, Ebay – always pay via the platform's website, delete unsolicited emails.
  - Super-realistic fake email.
- Spoofing
  Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.
  Spoofing can be used to gain access to a target's personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an advanced persistent threat or a man-in-the-middle attack.
- Trojans -- gives malicious users remote control over the infected computer. They enable the author to do anything they wish on the infected computer – including sending, receiving, launching and deleting files, displaying data and rebooting the computer.
- Unknown USB drive
- USB killer sticks

- Western Union and MoneyGram – be exceedingly wary of anyone wanting you to send them money, especially via Western union or MoneyGram.
- Zombies (bots), botnets

7.5 Protection

You can't be 100% secure. Don't rely on a single method of protection.

7.5.1 Protect your identity and privacy

- Use strong passwords.
- Keep personal data stored on Internet at a minimum. If trivial sites (eg loyalty card sites, Facebook) ask intrusive questions (like DOB) just lie (convincingly, Use January 1 in your year of birth – makes it easier for you to remember).
- Check your privacy settings on social media sites – eg Facebook, Linkedin.
- Do not use public computers and public Wi-Fi to access bank accounts, email, etc. Look at using portable software or a portable hotspot. To be safe, do not use public Wi-Fi for anything.
- Log out of websites when you are finished – especially if you are using a public computer or public Wi-Fi.
- Under no circumstances allow your device or web application to 'remember me'.
- Check account balances regularly – every day if possible. Keep a record of your own spending. Keep all receipts.
- Do not use links to access bank accounts (other than your own stored links).
- Do not share confidential information by email.
- Do not share holiday plans, photographs of your house, car or caravan, or any other information that might allow someone to identify you or where you live.
- If you MUST use a public Wi-Fi, use in conjunction with a VPN (Virtual Private Network). A VPN gives you online privacy and anonymity by creating a private network from a public internet connection. It masks your internet protocol address to keep your online actions private. It provides secure and encrypted connections to provide greater privacy and security.

7.5.2 Other steps

- Do not rely on a single product. No software is 100% perfect. You must remain vigilant:
    - Install MalwareBytes, CCleaner
    - Do not install ANY software that pops up and claims:
        1. to speed up your computer,
        2. to clean your computer of viruses and other malware, or
        3. offers to perform some other magic trick on your computer
- Don't give out passwords to anybody
- Don't reuse passwords
- PGP – Pretty Good Privacy or WhatsApp for encrypted messaging.
- Public key cryptography

- Security keys
- Security threats are regularly published in the press. Read and learn from them. Read security blogs.
- Set up bank accounts to alert you when transactions exceed a certain limit (eg $100)
- Use two-factor authentication whenever possible
- Vigilance
- When installing software, carefully inspect every window that pops up to be sure you are not installing other software that you don't want (eg another anti-virus)

7.6 Online payments

- Use a debit card (with just enough money on it) for online purchases.
- Use PayPal with 2FA (two-factor authorisation)
- Set up a separate savings account for PayPal

7.7 How to clean up a serious malware infection

- There's probably no easy solution depending on the scale of the infection.
- Make sure you have a reputable anti-virus (AV) installed and it is up-to-date,
- Install and run MalwareBytes
- As a last resort:
    - Back up all your data
    - Take a snapshot of your computer system using Belarc Advisor
    - Reinstall the operating system from your system disks
    - Allow your operating system to update itself
    - Reinstall your applications (listed in Belarc Advisor report)
    - Run a complete AV scan
    - Reinstall your data.
    - Run a complete AV scan again

7.8 Links

- http://belarc.com/free_download.html
- https://blog.threattrack.com/
- https://blogs.technet.microsoft.com/mmpc/
- http://cio.com/category/security
- https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers
- http://facecrooks.com/
- https://fixmestick.com/
- https://grc.com/
- http://howtogeek.com/233952/how-to-find-your-routers-ip-address-on-any-computer-smartphone-or-tablet/
- http://krebsonsecurity.com/
- https://mathsisfun.com/binary-number-system.html
- https://motherboard.vice.com/read/fake-gmail-alerts-phishing?utm_source=mbtwitter
- https://scamwatch.gov.au/
- https://staysmartonline.gov.au/
- http://theage.com.au/business/consumer-affairs/phishing-emails-and-other-online-scams-on-the-rise-as-australians-lose-millions-of-dollars-20161115-gspnar.html
- https://troyhunt.com/
- https://usbkill.com/
- https://us-cert.gov/
- https://westernunion.com/au/en/fraudawareness/fraud-be-aware.html
- https://www.howtogeek.com/58642/online-security-breaking-down-the-anatomy-of-a-phishing-email/

7.9 References

The Cracking Codebook, Simon Singh