==========

SCAM VICTIM - WHO TO RING AND WHAT TO DO

Prepared by Colin Clohesy at CoolTech Computers

==========

KEEP THIS SHEET. Work down it in order.

>>> STEP 1 - RING THE BANK RIGHT NOW <<<

Ring the number PRINTED ON THE BACK OF HER CARD. Not a number from an email, not from a popup, not from a text. The card is the only safe source.

If money has already gone, speed is everything. Banks can sometimes stop or recover a transfer if told quickly.

AUSTRALIAN BANK FRAUD / SCAM LINES

COMMONWEALTH BANK (CommBank)
Ring the number on the back of her card
Or in the CommBank app: Help and support > Report a scam
Web: commbank.com.au/security

WESTPAC
Fraud and scams ..... 132 032 (24 hours)
Report a scam text .... forward it to 0497 132 032
Web: westpac.com.au/security

ANZ
Customer Protection Team ... available 24/7
Ring the number on the back of her card, or in the ANZ app
Web: anz.com.au/security

NAB
Personal fraud and scam support 13 22 65
Web: nab.com.au/security

BENDIGO BANK / ADELAIDE BANK
Fraud 1300 236 344
Web: bendigobank.com.au/security

BANK OF MELBOURNE / BANKWEST / ST GEORGE / other
Ring the number on the back of her card. All banks have a 24/7 fraud line - ask for "fraud" or "scams" and they will transfer you.

CREDIT UNION / BUILDING SOCIETY
Ring the number on the card or the branch. Ask for their fraud team.

>>> STEP 2 - SUPPORT AND REPORTING (all free) <<<

IDCARE - * START HERE IF SHE'S UPSET ***
1800 595 160
Mon-Fri 8am-5pm
www.idcare.org

Australia's national identity and cyber support service. Free.
They are NOT a bank or a government department - they are counsellors who help scam victims make a plan and work through it. If she is embarrassed, overwhelmed, or doesn't know what to do next, this is the number for her. They handle exactly this, every day.

SCAMWATCH (ACCC)
www.scamwatch.gov.au/report-a-scam
Report the scam. Takes 5 minutes. Helps protect other people.

REPORTCYBER (Australian Cyber Security Centre)
www.cyber.gov.au/report-and-recover
Report the cybercrime itself. Gives her an official reference number, which the bank may ask for.

AUSTRALIAN CYBER SECURITY HOTLINE
1300 292 371 (1300 CYBER1)
For advice if she's unsure whether something is a scam.

VICTORIA POLICE
131 444 (non-emergency)
000 (if she is in immediate danger)
Report the fraud. Useful if the bank needs a police report.

LIFELINE
13 11 14 (24 hours)
Being scammed is a shock. This is free and confidential.

BEYOND BLUE
1300 22 4636

>>> STEP 3 - CHANGE PASSWORDS (DO THIS FROM HER PHONE) <<<

***** NEVER on the computer that was scammed. Use her phone or my laptop. *****

IMPORTANT: changing a password is NOT enough on its own. A scammer who took a logged-in session stays logged in. Every change must also include:
"SIGN OUT OF ALL DEVICES / ALL SESSIONS"

ORDER:

1. EMAIL first (it's the reset link for everything else)
   - change the password
   - sign out of all other devices
   - turn on 2-factor
2. BANKING and payment apps
   - change password, sign out all devices
3. Anything saved in her browser:
   chrome://password-manager/passwords
   (or edge://settings/passwords)
4. Other email / social / shopping accounts
5. Turn on 2-factor everywhere it's offered

>>> STEP 4 - TELL HER THESE THREE THINGS <<<

---

1. "It is NOT your fault. This is a professional operation that targets thousands of people every week. They do it for a living."

2. "The bank and IDCARE deal with this every day. You are not the first and you won't be the last - and they will help you."

3. "The computer is cleaned. What keeps them out from now on is your passwords, changed from your phone. Let's do that now."

==========

WHAT WE DID ON YOUR COMPUTER

[ ] Swept the machine for remote-access software and removed what we found
[ ] Checked everything that starts automatically
[ ] Checked scheduled tasks, services and user accounts
[ ] Checked the web browser - history, extensions and saved logins
[ ] Checked for anything installed or created around the time of the scam
[ ] Ran antivirus scans

Findings: _____
_____
_____

Date of visit: _____

***** WHAT WE CAN AND CANNOT PROMISE *****
The remote access is removed and verified. We cannot prove what was taken - no one can, because this type of software takes data and leaves nothing behind. What stops them getting back in is your passwords, changed from a different device. That is the step that matters most.

==========

Prepared by

Colin Clohesy ..... CoolTech Computers

Date: _____

==========