Customer Education

Spam Call Information

Scam phone calls or unwelcome calls

Telephone-based scam callers often claim to be from well-known organizations such as AAPT Business Connect, the Government, or other brands or organisations you're likely to have heard of. These scam callers will often try to convince you of the urgent need to follow their instructions. Sometimes they will try to convince you to give them access to your computer remotely, such as when pretending to be an NBN employee. Often, they will apply inappropriate pressure, including threats and potentially inappropriate language, as part of their scam.

What to look out for:

- Calls from people impersonating employees from well-known organisations, such as the Government, or familiar brands and companies.
- Calls seeking financial details, such as your credit card or banking details, in order to process a refund or other 'overpayment'.
- Callers which attempt to apply a lot of pressure, urging you to take immediate action to address a problem.
- Callers advising that your computer has a virus or is attacking others.
- Please note, we won't request confidential information over the phone. Any requirement will be in writing from an @aaptbc.com.au domain.

Example of scam phone calls

- Calls asking for bills to be paid via prepaid gift cards – such as iTunes and Westfield – on behalf of a credit agency representing AAPT Business Connect or the Australian Taxation Office (ATO).
- Calls imitating support desk staff looking to access your computer by pretending to know your CLSID. This is a non-unique identifier which scammers try to pass off as something only a legitimate support person would know.

What to do next:

- If you're not sure that the person on the other end of the phone actually is who they say they are, hang up and call the organisation by using their official published contact details.
- If the caller is claiming to work for AAPT Business Connect, do not share your personal information, credit card or online account details over the phone, unless you made the call and the number you called came from a trusted source, such as the contact details provided on your bill.
- Don't respond to missed calls from numbers you don't recognise. Calling back may result in instant charges in excess of $20.
- Be wary of phone numbers beginning with '190'. These are charged at premium rate and can be expensive.
- Be careful of being tricked into calling expensive international phone numbers.
- changing PINs and passwords regularly; selecting strong PINS and passwords.
- contacting your financial institution immediately if they believe they have lost money to a scammer
- Reporting the scam to www.scamwatch.gov.au.

A life-threatening communication is more serious and involves the use of a carriage service connected with an event which gives a person reasonable grounds to believe that there is a serious and imminent threat to a person's life or health. If you are receiving life threatening communications please report these to the police immediately.

If you have received only one or two unwelcome communications we are limited in our ability to assist. However, if you have received a 'pattern' of unwelcome communications there are set protocols established that sets out how we can handle these

Step 1: Please provide a pattern of unwelcome communications:

(a) ten or more unwelcome communications in a 24-hour period;
(b) three or more unwelcome communications that are spread over a period of more than 24 hours and less than 120 hours; or
(c) unwelcome communications made at consistent and/or regular intervals

Customer Education

Spam Call Information

Step 2: Contact AAPT Business connect with call data

Contact us: **support@aaptbc.com.au** or **1300 227 822**

Step 3: Investigation

We'll investigate to see whether a pattern of unwelcome communications has been established.

If it has, with your consent, we'll contact the service provider that supplies the service to the party that's initiating the unwelcome communications. That service provider will be responsible for issuing warning letters to the individual responsible for the unwelcome communications.

If the unwelcome communications continue after 2 warnings, a third and final warning is sent and then additional options are available, including suspending or disconnecting the service being used to make the unwelcome communications.

If at any stage during this process you continue to receive unwelcome communications, you should keep recording the details of these communications as set out in Step 1 and report them to us.

Important:

- Any action taken by AAPT Business Connect is under strict guidelines that are set out in the **Communications Alliance Code**
- There are some limitations on AAPT Business Connect' ability to address unwelcome communications (e.g. in a situation where the identity of the individual initiating the unwelcome communications cannot be established)
- The exchange of information between service providers to investigate unwelcome communications is governed by the **Industry Code**
- An **Industry Guidance Note** has been developed with more information for customers about the management of unwelcome communications

Telemarketing calls

If you don't wish to receive telemarketers' calls, you can add your number to the Australian Communications and Media Authority's (ACMA) **'Do Not Call Register'**. It may take up to 30 days for marketing agencies to recognise your registration and stop calling you. Mobile numbers remain on the register indefinitely. You can **remove your number from the register** if your situation changes.

Adding your number should stop most unsolicited calls but some categories of callers such as charities or religious organisations, registered political parties, educational institutions, market researchers and companies you have an active ongoing business relationship with will still be able to call you.

Where can I find more information?

- **ACCC Scamwatch**
- **ACSC Stay Smart Online program**
- **ACMA Phone Scams website**
- **ATO Scam Alerts**
- **Services Australia - Scams and Identity Theft**
- **ACCC Little Black Book of Scams**