Image: sam-carter-GHOiyov2TSQ-unsplash (cropped)

Dr. Terence Love CEO at the Design Out Crime & CPTED Centre.

June 6, 2020

Fleece-ware - cybercrime or not?

Fleece-ware is a new category of cyber-scam that is partly in the digital world and partly in the physical world.

It works by:

- Having YOU agree to pay outrageous amounts of money for things you are buying online when you think you are paying much less.
- It arranges that you agree to pay much more than you thought.

Fleece-ware is different from cyber-crime because much of it is absolutely **legal**.

How does fleece-ware work?

The fleece-ware operators use buyers' carelessness, trust and lack of attention to the purchase details to arrange that the buyer will legally agree to pay more than they thought they were paying.

Examples:

1. A phone app worth about $20 is very visibly priced at $20.00 elsewhere on a website but in the checkout section itself the price agreed by the buyer is $200.0. It relies on people being unaware, or overly trusting, thinking something must be a typo - and then still making the legal agreement to pay.
2. Many people don't read the small print or the terms. The terms of an app or product might seem to be $20 and that was actually $200.0 *might also include in the terms that the agreed $200 is "to be paid monthly"*. If you pay by PayPal or card and don't notice that a subscription has been set up, that payment will go out every month.
3. You notice they charged you too much and you noticed the subscription, so you deleted the app? However, the payment on the subscription keeps paying out because it was agreed to...

Conventional malware protection does not block fleece-ware.

Malware protection may be in place, firewalls secure, software all up to date - all the usual cyber-security protection to the best standard.

None of the anti-malware and cyber-security software stop fleece-ware.

For fleece-ware it is **the buyer that is the weak link** - the vulnerability

Fleece-ware is typically not doing anything illegal. It asks that a certain price be paid, and the buyer agrees to it.

Fleece-ware uses standard formats and settings.

Tom Merritt in Tech Republic points out it does this,

"To fool you into agreeing to high charges without realizing it until it's too late. For instance, it will give you a free trial with a subscription price of $9 a week, hoping you don't notice that it was a week, not a month. Or they may charge you $200 a month hoping you'll read it as $2.00."

In most cases, **everything is legal but different from what the buyer is expecting.**

Companies know buyers have a lack of attention to agreements and trust too much

Fleece-ware preys on the buyer's trust and lack of attention in agreeing to a deal that is more expensive than they think.

Many software companies have tested buyers' lack of attention in their terms of trading - some humorously.

For example, Gamestation apparently included the clause that buyers would be required,

"...to grant Us a non-transferable *option to claim, for* now *and for ever more, your immortal soul. Should We wish to exercise this option, you agree to surrender your immortal soul, and any claim you may have on it, within 5 (five) working days of receiving written notification from gamestation.co.uk or one of its duly authorized minions."*

Note: Only 12% of purchasers ticked the clause to "nullify soul transfer"

(GameStation has graciously relinquished their rights to the souls).

Amazon apparently also once had a clause in their terms that negated a section in their agreement as follows,

"However, this restriction will not apply in the event of the occurrence (certified by the United States Centers for Disease Control or successor body) of a widespread viral infection transmitted via bites or contact with bodily fluids that causes human corpses to reanimate and seek to consume living human flesh, blood, brain or nerve tissue and is likely to result in the fall of organized civilization."

Protection against Fleece-ware

The most obvious protection as a buyer is to never trust sellers. Check everything!

Part of this is to increase one's level of attention to all aspects of the transaction.

Do the hard work of reading what is being agreed to and being sure NEVER to agree to something that you are unsure or trusting about.

One motto is 'If in doubt, don't pay out!'.

Other protections against fleece-ware include:

- Cancel and stop the process as soon as you have discovered any problem.
- Cancel all subscriptions for the product.
- Use PayPal or a similar service that offers protection against potentially misleading product advertising.
- Use consumer protection advice and laws against misleading contracts.
- Buy from marketplaces that offer indemnity against misleading transactions, or at least a cooling off period that gives buyers chance to discover the problem.

Cyber-CPTED and Fleece-ware

There are many new kinds of crimes such as fleece-ware that occur at the border of the digital and physical worlds.

Protection is gained against these new bodies of crime by a completely new kind of Crime Prevention Through Environmental Design (CPTED) that spans between physical crime prevention by CPTED and the digital territory of cyber-security - and which neither alone do well.

I have called this new body of crime prevention strategies -C***yber-CPTED***

3 years ago, I started building a new body of cyber-CPTED crime prevention methods that extend CPTED into the new crimes of the digital-physical crime space.

One area of the cyber-CPTED world started with some work addressing the security issues of ultra-high-value micro-businesses that operate in part in the digital world.

These are businesses with very few staff (2-5 typically) that handle transactions of very high financial value for high value businesses and individuals.

It quickly became clear that security and crime prevention in this mixed digital-physical realm must combine CPTED, security and cyber-security approaches in ways that go beyond any of them.

In cyber-CPTED situations, traditional principles of CPTED simply do not work.

For example, traditional natural surveillance is problematic in the cyber-CPTED realm. Do you really want everyone naturally being able to see all the files in your computer and your banking details...?

Similarly, many cyber-security approaches are also useless in a digital-physical realm because they do not apply to the physical aspects of the crime or are legal in the physical world (e.g. fleece-ware).

This new body of practical ***cyber-CPTED*** crime prevention methods will be published soon.

In the meantime, if you are a business, local government or other organisation who would like training in cyber-CPTED, please contact me. Contact details are at end of article.

References

https://www.techrepublic.com/article/top-5-things-to-know-about-fleeceware/?ftag=TRE684d531&bhid=28081711049292795333218934793615&mid=12845183&cid=2033187217

https://www.wired.com/story/what-is-fleeceware-protect-yourself/

https://www.groovypost.com/howto/what-is-fleeceware-and-how-do-i-protect-myself/

https://news.sophos.com/en-us/2020/01/14/fleeceware-apps-persist-on-the-play-store/

https://www.securemac.com/blog/what-is-fleeceware

https://www.onelegal.com/blog/fantastic-clauses-hidden-in-contracts-and-eulas/

CPTED Training, CPTED reviews and consultation

The **Design Out Crime and CPTED Centre** provides these articles as **free CPTED resources** for CPTED and Design Out Crime professionals.

Please see our website at www.designoutcrime.org or contact **Dr Terence Love** directly at t.love@designoutcrime.org and +61 (0)4 3497 5848 for in-person and online CPTED training for individuals and groups, for CPTED reviews for development applications and CPTED consultation for local government, developers and other professionals

A version of this article was first published on June 6, 2020 on LinkedIn at https://www.linkedin.com/pulse/fleece-ware-cybercrime-dr-terence-love