BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

November 2015 | Briefing 11

BUYERS BEWARE!

BLACK FRIDAY AND CYBER MONDAY SCAMS ARE AIMING AT YOU.

Only 47 shopping days before Christmas! But only 27 days before the biggest cyber crime season of the year – **Black Friday and Cyber Monday. This is the time of the year when online criminal activity peaks.** From bogus online deals and scams, to charges run up on stolen credit cards, and everything in-between, this is the time of year when the crooks who prey on consumers try to cash out. From now through the New Year, you need to go on high "cyber alert". **Follow these simple rules to stay safe during the online shopping season.**

1) IF IT LOOKS TOO GOOD TO BE TRUE, IT PROBABLY ISN'T TRUE.

Just like the $50 "Rolex" you can buy on the street, odds are that **the $10 Nikon Camera advertised in that email isn't really a Nikon**. Something else is going on. Don't fall for it. Don't click on that link. In other words, when you are presented with a link in an email, a paid ad, a social media post or a tweet, ask yourself, "Who sent that?" and "Why did I get that?" If you're not sure of the answers, don't click it. **In fact, just don't click.**

WHAT BRANDPROTECT LEARNED LAST YEAR

Email schemes grew steadily throughout November, peaked on Cyber Monday and continued strong into the first week of December. BrandProtect detected an average of more than 2000 different active scams every day from mid-November through December 1, 2014.

MOBILE APP SCAMS UP

300%

Compared to 2013, malicious mobile app activity skyrocketed 300% in 2014. Over 3100 apps targeting Black Friday and Cyber Monday shoppers were identified.

Facebook and Twitter were heavy channels for fraud and fraud alerts – there were literally hundreds of thousands of posts. Combined, over 90% of all fraud and fraud alert social media activity took place on Facebook or Twitter. Twitter mentions grew 40% from 2013 to 2014. BrandProtect did not measure Instagram in 2014.

YOU CAN NEVER BE TOO SAFE

2) DOES THE EMAIL MAKE SENSE?

A rapidly emerging criminal ploy are **emails that look like they are coming from someone you know**. When an email account is compromised, so is the address book. When a phone or tablet is infected with certain kinds of malware the bad guys get a copy of the contacts saved on that compromised device. With this information, they can send out emails to people that seem to be from someone you know, someone you trust. The bad guys can then send out very convincing emails to those stolen contacts that look like they are coming from the compromised individual. So, if your bowling buddy is urging you take advantage of great prices for luxury coffee makers, something might be wrong.

3) SHOP ONLY AT THE PLACES YOU TRUST.

The scammers are clever – they will build sites that are almost exact copies of legitimate corporate sites, using the correct colors, fonts, logos, everything. Only the URL will be incorrect. You'll think you are someplace you are not. The easiest solution? Type in the name of the site you know, not "Nikon-on-sale.com" but "www.nikon.com." The deals that look the best might be on some pretty dangerous sites.

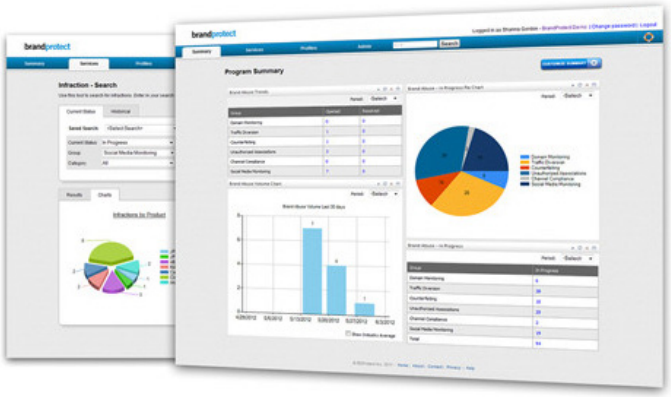
4) DON'T TRUST ONLINE ADS

Scammers Advertise! One of the fastest growing consumer attacks involves very convincing pop-up and online banner advertisements purchased by the bad guys and targeted to your user profile. **Try to resist clicking on the ad – it can be just as dangerous as a link in an email**. Instead, read the ad and close it. Then go the manufacturer's or reseller's page and look for the deal there.

IT'S NOT JUST YOU, IT'S YOUR FAMILY TOO

One of the things that makes this season so attractive to criminals is that for a few weeks, shopping becomes a kind of national sport. Everyone is shopping for everyone. The rules that apply during the rest of the year are relaxed so that the shopping can get done (children are given permission to use credit cards, purchases are made "in secret," etc…) **It doesn't matter whether it is your misstep or your child's misstep.** The deal you want to avoid is the one where the criminals gain access to your accounts or your identity. Make sure that everyone is being careful.

WHAT CAN A BUSINESS DO?



If your firm isn't already proactively monitoring for phishing attacks, social media, auction sites, and online masquerades that leverage your trusted brand name, now is a great time to start. As a BrandProtect client puts it, "My job is to make sure that whenever a customer or prospect clicks on a link that carries our trusted name, I want to be sure that they are going someplace safe, to a site that we control or authorize."

Companies that monitor and mitigate online fraudsters become harder targets, and are less attractive targets for fraudsters. The process of online threat and risk monitoring is easy to begin, and reduces the risk that your corporate reputation is tarnished by a third-party scheme. **Contact us if you would like to know more.**

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725

For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.