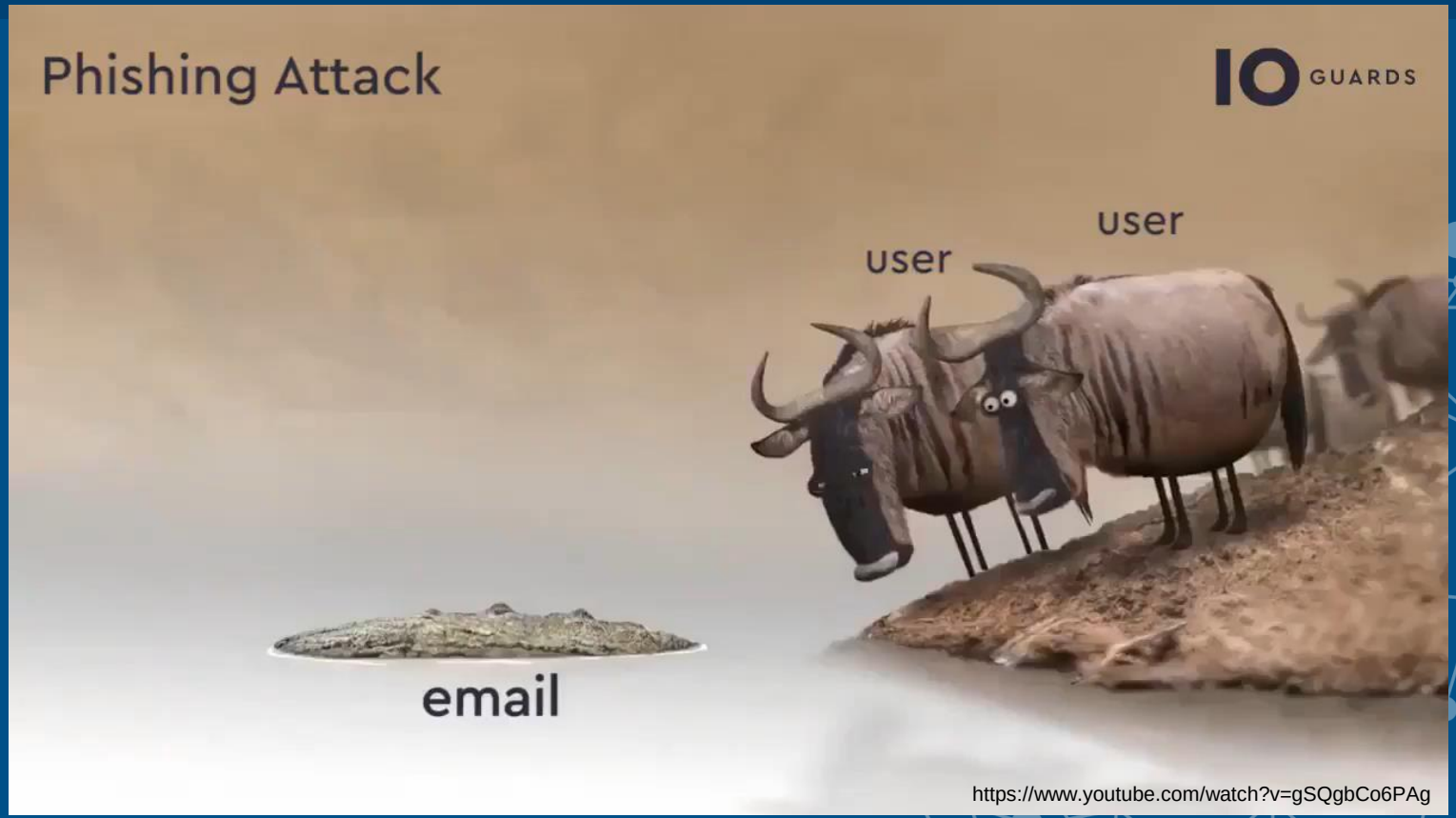
IP Telecom

Cibersegurança @ IP Telecom

Análise de Emails

IP Telecom
Ligamos Negócios

cloudsolutions


Phishing Attack
IO GUARDS
user
user
email
https://www.youtube.com/watch?v=gSQgbCo6PAg

Estatísticas de CiberAtaques

IP Telecom

43%
were social attacks
(somebody used a social tool, such as email for the attack)[5]

51%
included malware
(somebody installed unauthorized software)[5]

62%
of breaches featured hacking
(somebody attained unauthorized access)[5]

37.6%
of the breaches used desktops as the conduit to compromising data[6]

32.3%
of the breaches used people as a means to compromise data[6]

27%
were discovered by third parties
(somebody outside of the organization informed them that they were breached)[4]

66%
of malware was installed via malicious email attachments[5]

81%
of hacking-related breaches leveraged either stolen and/or weak passwords
(somebody used unauthorized access to steal credentials and then installed unauthorized software)[5]

https://secure.wphackedhelp.com/blog/remove-phishing-wordpress/

IP Telecom

280 days

the average time to indetify breach in 2020

$1 million

Average savings from containing a breach in less than 200 days

$150

Customer PII data has the highest cost per record

$3.86 M

Global average total cost of a data breach in 2020

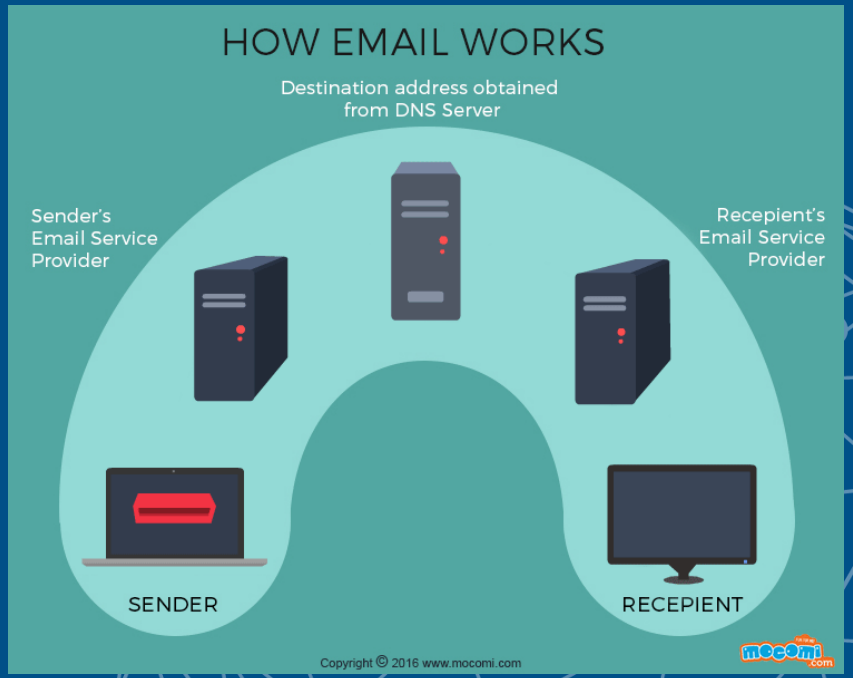
https://dataprivacymanager.net/100-data-privacy-and-data-security-statistics-for-2020/

IP Telecom

Arquitetura de um Email

Como funciona o email

- MUA (Mail User Agent)– Outlook, Gmail;
- MTA (Message Transfer Agent) – POP3, IMAP;
- MDA (Mail Delivery Agent) – Dovecot, maildrop.



IP Telecom

Phishing

Phishing – Método de "ataque"

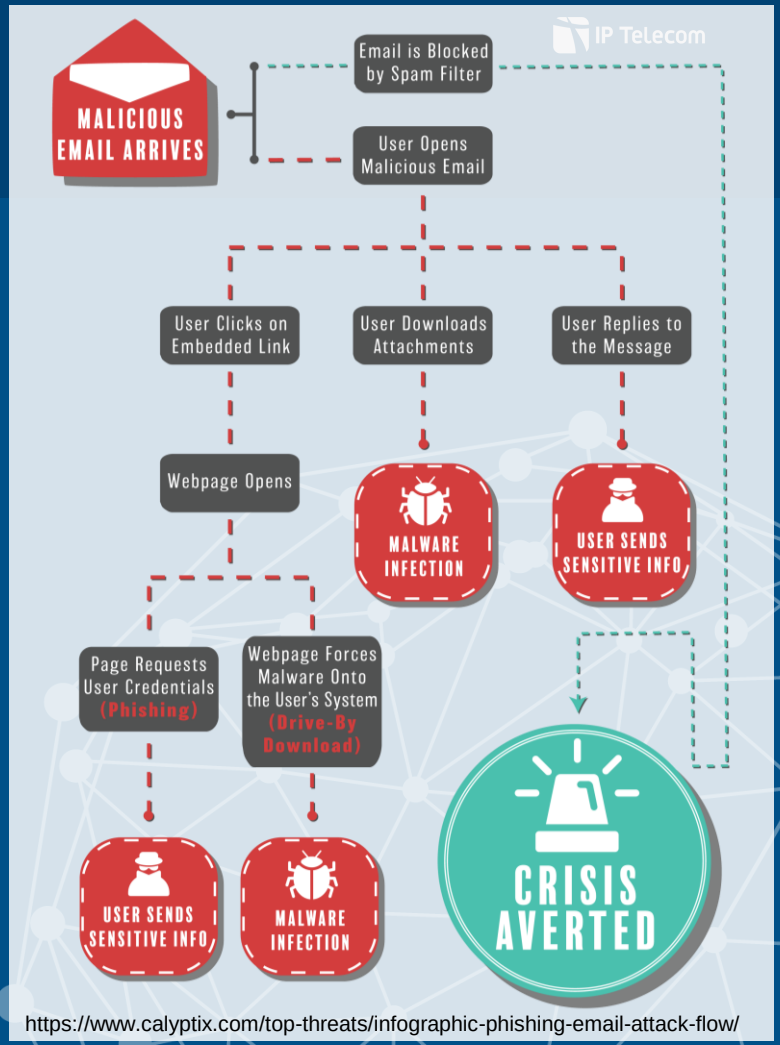
phishing

nome masculino

atividade criminosa que consiste em enviar emails não solicitados cujo objetivo é induzir o utilizador a fornecer dados pessoais e/ou financeiros

https://www.infopedia.pt/

- O ataque é realizado por meio de comunicações eletrônicas, como e-mail.
- O criminoso finge ser um indivíduo ou organização de confiança.
- O objetivo é obter informações pessoais confidenciais, como credenciais de login ou números de cartão de crédito.



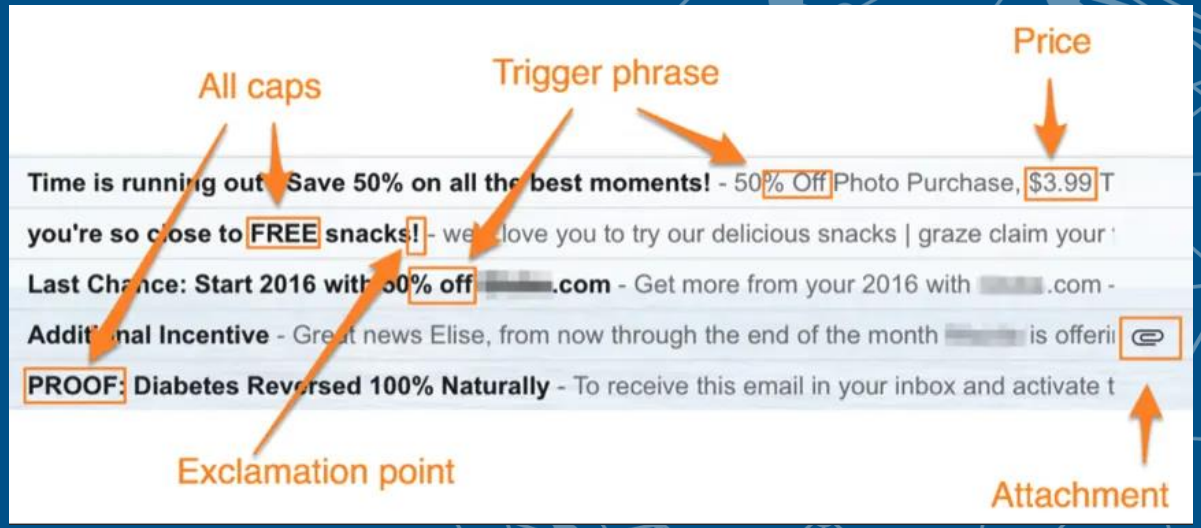
https://www.calyptix.com/top-threats/infographic-phishing-email-attack-flow/

IP Telecom

Tipos de Emails de Phishing

Spam

- Mensagem não solicitada;
- Intuito de chegar ao máximo de utilizadores possíveis;
- Muito focado em marketing de produtos;
- Aliado a técnicas de phishing pode ser perigoso.



Roubo de Credenciais

1. É enviado um email de phishing;
2. O utilizador é encorajado a carregar num link e efetuar uma ação;
3. O link encaminha para uma página web (maliciosa);
4. O utilizador é aliciado a colocar o seu email e a password ou outra informação pessoal;
5. O utilizador malicioso no final recolhe os dados da página web.

Engenharia Social

- Manipulação do utilizador para atingir um objetivo;
- Um exemplo é fazer-se passar por um membro da equipa de TI;
- Permite ao utilizador malicioso obter dados sensíveis sobre a organização.

IP Telecom

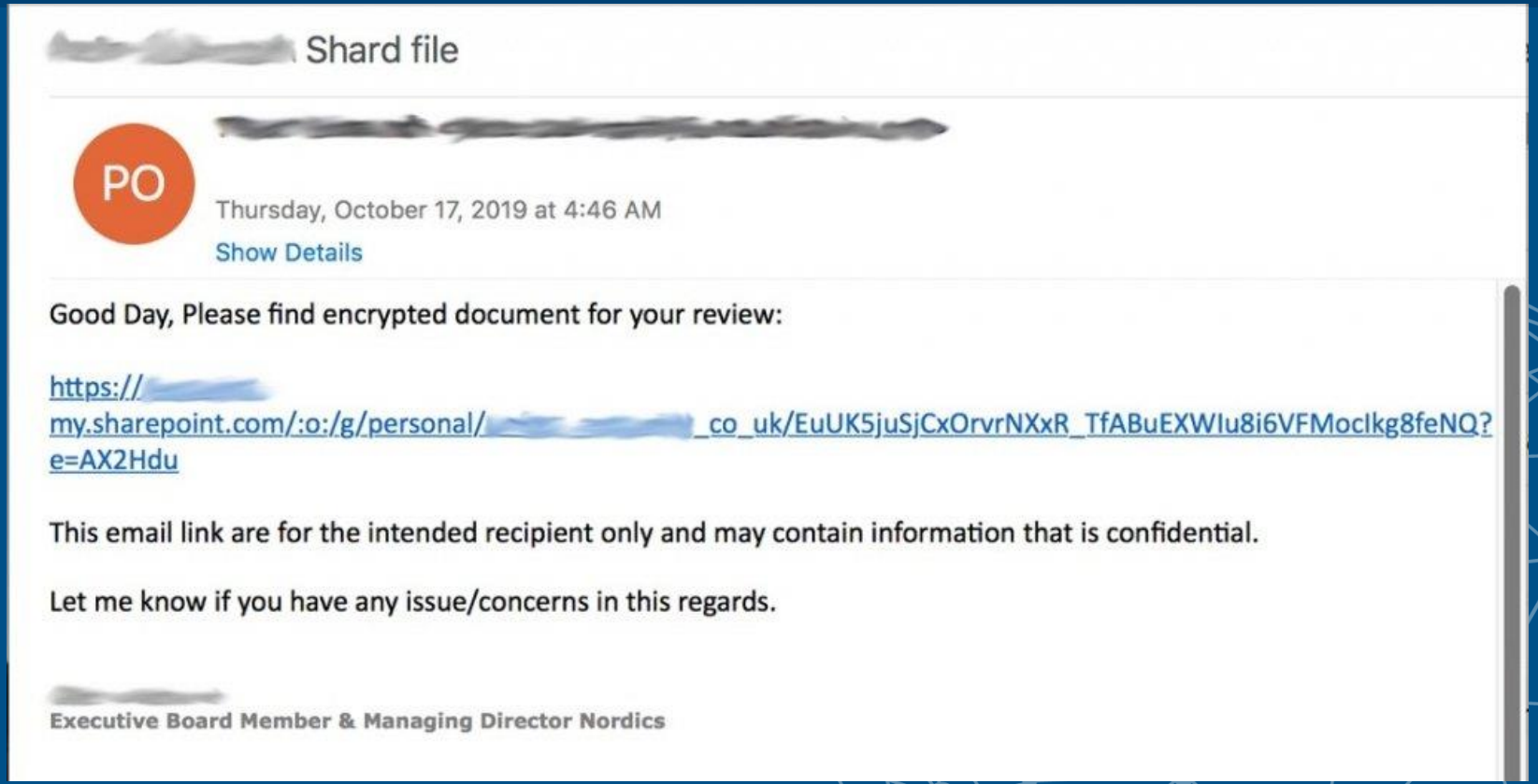
Táticas e Técnicas de Emails de Phishing

Spear Phishing

- Focado apenas num grupo minoritário;
- É um ataque mais personalizado;
- Focado apenas nas organizações;
- Envio de emails em nome de uma entidade credível;

Exemplo de Spear Phishing

IP Telecom



[redacted] Shard file

PO

[redacted]

Thursday, October 17, 2019 at 4:46 AM

Show Details

Good Day, Please find encrypted document for your review:

https://[redacted]
my.sharepoint.com/:o:/g/personal/[redacted]_co_uk/EuUK5juSjCxOrvrNXxR_TfABuEXWIu8i6VFMocIkg8feNQ?e=AX2Hdu

This email link are for the intended recipient only and may contain information that is confidential.

Let me know if you have any issue/concerns in this regards.

[redacted]

Executive Board Member & Managing Director Nordics

Clone Phishing

- Mais difícil de ser detetado;
- O email malicioso é replicado através de um email verídico;
- Corpo da mensagem igual ao do email original;
- Apenas difere na inclusão de um link ou anexo;

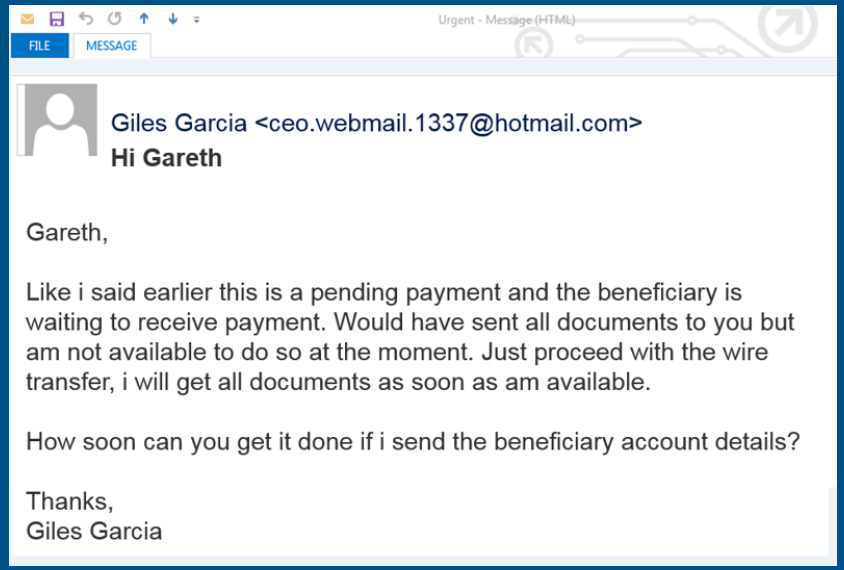
Sent from an email address spoofed to appear to come from the original sender

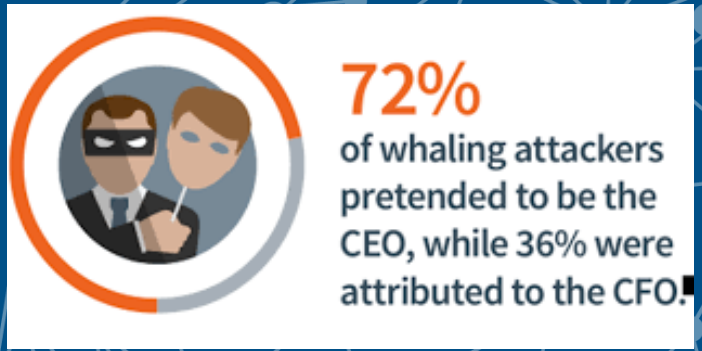
The attachment or link within the email is replaced with a malicious version

It may claim to be a re-send of the original or an updated version to the original.

Whaling

- Os alvos são colaboradores com cargos executivos;
- Objetivo é enganar membros da administração ou diretores de departamentos;
- *Leak* de informação sensível;
- Requer uma pesquisa intensiva por parte do utilizador malicioso.





Exemplos de Whalling

IP Telecom

Whaling Attacks Real Cases

Whaling attacks are breathtakingly simple in planning and execution and can bring the rich promise of big rewards which is leading them to become a highly favored method of social engineering attacks. As these phishing style attacks are so personalised and targeted they are very difficult to identify and record.

Snapchat

This social media messaging giant fell victim to a concerted whaling attack in 2016. Despite it being company policy NOT to open on click on suspicious, phishing looking emails someone did, and cyber carnage resulted

B. Pathe

Pathe as they became a victim of BEC (Business Email Compromise) whaling attack when the CFO received a phishing email which led to their Dutch subsidiary eventually losing €19 million ($21.5 million).

FACC

The Austrian airplane parts supplier FACC was the victim of one of the biggest cyber crimes to hit the corporate world. In 2018, a staggering 50 million Euros (54 million US Dollars) was siphoned off in a fraudulent cyber attack.

Evil Twin

- Executado através de uma rede *Wifi* falsa;
- Mascara-se de uma rede verídica;
- Permite obter dados de contas, passwords e anexos;

Watering Hole

- O atacante compromete um website;
- O utilizador acede a esse website comprometido;
- Após esse acesso, é descarregado um malware;
- É possível descarregar dados de pessoas e/ou organizações:
  - Informações pessoais,
  - Dados financeiros,
  - Credenciais ...

Ofuscação de Endereços Web

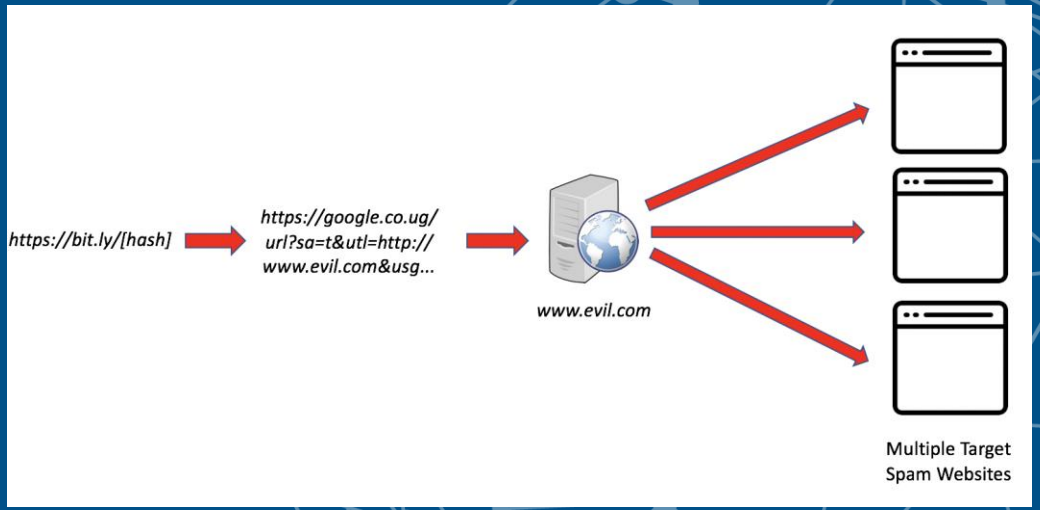
- Tem como objetivo não apresentar o url de destino final;
- Pode ter várias camadas;
- Serviços como o tinyurl.com, bit.ly e o goo.gl fornecem esse tipo de ofuscação;
- Alguns filtros de spam já bloqueiam este tipo de endereços.

Como pré-validar um endereço "curto":

tinyurl.com entre "http://" e o "tinyurl," escrever **preview.**
Exemplo: http://preview.tinyurl.com/zn7xnzu

bit.ly no fim do URL, adicionar o simbolo **+**.
Exemplo: http://bit.ly/2lgPesi+

goo.gl no fim do URL, adicionar o simbolo **+**.
Exemplo: https://goo.gl/vLfoaW+



IP Telecom

Como detetar um email Malicioso

Boas Práticas contra o Phishing

- Verificar o endereço de email emissor;
- Analisar a ortografia do email;
- Caso existam links no email, verificar a sua autenticidade através da leitura do url;
- Basta apenas existir a troca de um caractere e o endereço de email pode parecer credível;
- Anexos suspeitos podem indicar um email malicioso;
- Elevada urgência na reposta, pode indicar sinais de um email malicioso.

Detecting a Phishing Email

LogRhythm Labs

10 Things to Watch

With the uptick in ransomware infections that are often instigated through phishing emails, it's crucial to take proactive measures to help protect yourself and your organization's security.

Having a computer that is up to date and patched makes a big difference in reducing an organization's overall risk of infection.

But being vigilant in detecting phishing emails and educating employees in your organization to also be proactive is a critical step in protection.

Here is a quick top ten list for how to spot and handle a phishing email.

1 Don't trust the display name of who the email is from.

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.

2 Look but don't click.

Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.

3 Check for spelling errors.

Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

4 Consider the salutation.

Is the address general or vague? Is the salutation to "valued customer" or "Dear [insert title here]?

5 Is the email asking for personal information?

Legitimate companies are unlikely to ask for personal information in an email.

6 Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

7 Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails.

8 Be careful with attachments.

Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.

9 Don't believe everything you see.

If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).

10 When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than than to put the organization at risk.

Copyright © April 2016, www.logrhythm.com

Exemplos de “Phishing”

Exemplos de Emails de Phising

IP Telecom

Santander NEGOCIOS & EMPRESAS

Prezado Cliente Santander Empresarial

Após uma análise em nossos sistemas, identificamos que Habilitação do ID dispositivo encontra-se com erros em sua aplicação, causando assim, falhas no acesso ao Santander Internet Banking ..

Para solucionar esse problema, realize a autenticação do seu certificado.

CONFIRMAR

O Banco Santander garante o sigilo dos seus dados. Acesse o site do Banco Santander e conheça a nossa política de privacidade. Por favor, não retorne este e-mail. Para contatar, utilize o Fale Conosco do site do Banco Santander . Dúvidas, reclamações e sugestões: vá à sua agência, ligue para o SAC Santander (0800 728 0728), SAC Santander exclusivo ao deficiente auditivo e de fala (0800 722 1722) ou acesse o Fale Conosco (www. santander .com.br). Se não for solucionado o problema, utilize a Ouvidoria Corporativa Santander : 0800 570 0011, em dias úteis das 9h às 18h, ou Caixa Postal 67.600, CEP 03162-971. Esta mensagem eletrônica é confidencial. Sua utilização, cópia, distribuição ou divulgação são expressamente proibidas, sob pena de responsabilização civil e criminal.

caixadirectaoperacoes@cgd.pt

Envio de comprovativo

Não abra o anexo!
Pode infetar o seu computador/dispositivo com software malicioso.

To caixadirectaoperaces@cgd.pt

Attachments COMPROVATIVO.PDF.tar (1 MB)

If there are problems with how this message is displayed, click here to view it in a web browser.

Anexo fraudulento

Caixadirecta Empresas

Exmo(a) Sr(a)

Na sequência do pedido efectuado por [redacted], enviamos em anexo o comprovativo de registo da operação **Transferência SEPA nacional**, efectuada no serviço Caixadirecta Empresas.

Sobre esta operação [redacted] envia-lhe ainda o seguinte comentário:
PGT FACTURA [redacted]

Caso necessite de obter alguma informação adicional, contacte o serviço Caixadirecta Empresas pelo telefone 707 24 24 77 (das 8.00h às 22.00h / todos os dias do ano).

Caixadirecta Empresas
Na Caixa. Com certeza.

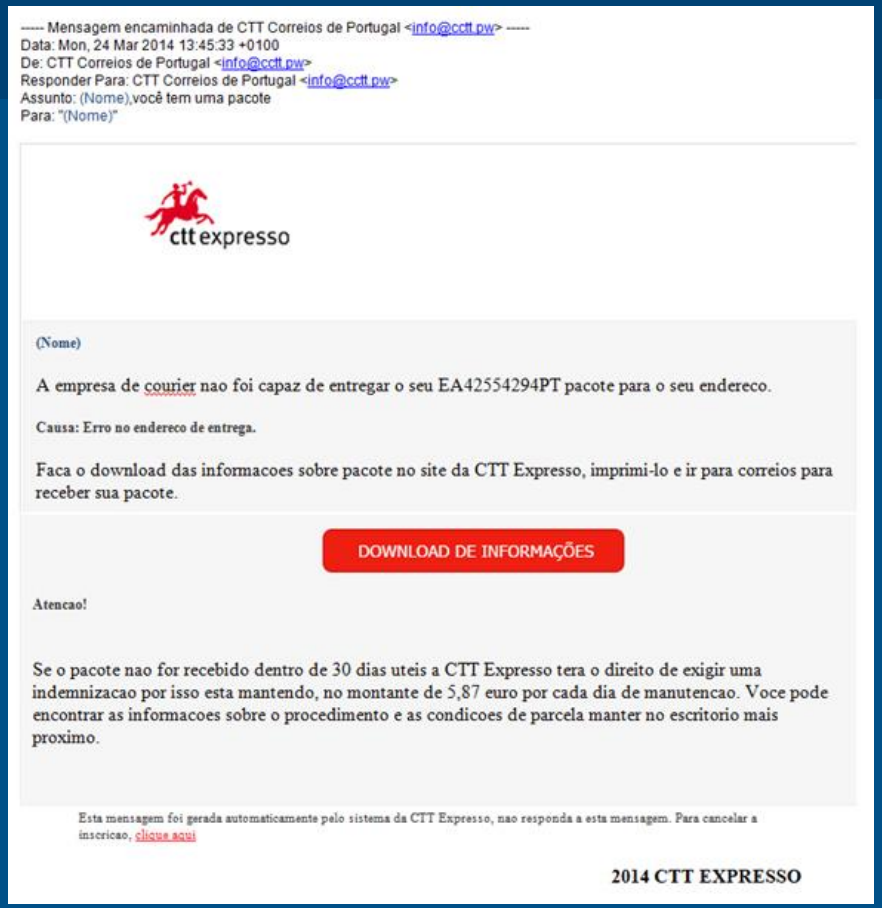
Nota:
Esta comunicação foi enviada automaticamente.
Por favor não responda a este e-mail, porque a caixa de correio destina-se exclusivamente ao envio de correio electrónico.
Para mais esclarecimentos sobre esta comunicação será necessário contactar o ordenante da operação.

AVISO LEGAL
A informação presente nesta mensagem, bem como em qualquer dos seus anexos é confidencial e destinada exclusivamente ao(s) destinatário(s). Qualquer utilização desta informação que não esteja de acordo com o seu objectivo, qualquer disseminação ou divulgação, total ou parcial, é proibida excepto se formalmente aprovada. A Internet não garante a integridade desta mensagem, a qual poderá ter sido interceptada, corrompida, perdida, atrasada ou acrescida de vírus. Assim, a Caixa não se responsabiliza pela mensagem se modificada.

FRAUDE

Exemplos de Emails de Phising

IP Telecom



----- Mensagem encaminhada de CTT Correios de Portugal <info@cctt.pw> -----
Data: Mon, 24 Mar 2014 13:45:33 +0100
De: CTT Correios de Portugal <info@cctt.pw>
Responder Para: CTT Correios de Portugal <info@cctt.pw>
Assunto: (Nome),você tem uma pacote
Para: "(Nome)"

ctt expresso

(Nome)

A empresa de courier nao foi capaz de entregar o seu EA42554294PT pacote para o seu endereco.

Causa: Erro no endereco de entrega.

Faca o download das informacoes sobre pacote no site da CTT Expresso, imprimi-lo e ir para correios para receber sua pacote.

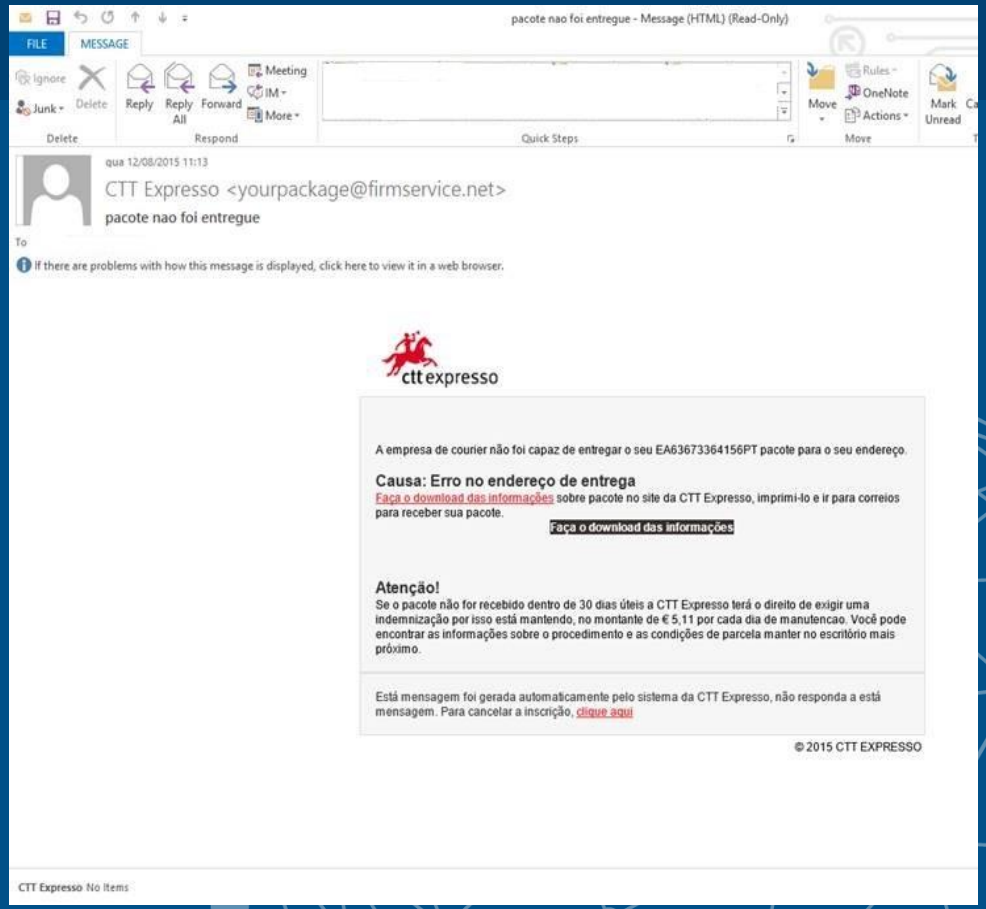
DOWNLOAD DE INFORMAÇÕES

Atencao!

Se o pacote nao for recebido dentro de 30 dias uteis a CTT Expresso tera o direito de exigir uma indemnizacao por isso esta mantendo, no montante de 5,87 euro por cada dia de manutencao. Voce pode encontrar as informacoes sobre o procedimento e as condicoes de parcela manter no escritorio mais proximo.

Esta mensagem foi gerada automaticamente pelo sistema da CTT Expresso, nao responda a esta mensagem. Para cancelar a inscricao, clique aqui

2014 CTT EXPRESSO



pacote nao foi entregue - Message (HTML) (Read-Only)

FILE MESSAGE

Ignore Junk Delete Reply Reply All Forward Meeting IM More Delete Respond Quick Steps Move Rules OneNote Actions Mark Unread Move

qua 12/08/2015 11:13

CTT Expresso <yourpackage@firmservice.net>

pacote nao foi entregue

To

If there are problems with how this message is displayed, click here to view it in a web browser.

ctt expresso

A empresa de courier não foi capaz de entregar o seu EA63673364156PT pacote para o seu endereço.

Causa: Erro no endereço de entrega

Faça o download das informações sobre pacote no site da CTT Expresso, imprimi-lo e ir para correios para receber sua pacote.

Faça o download das informações

Atenção!

Se o pacote não for recebido dentro de 30 dias úteis a CTT Expresso terá o direito de exigir uma indemnização por isso está mantendo, no montante de € 5,11 por cada dia de manutencao. Você pode encontrar as informações sobre o procedimento e as condições de parcela manter no escritório mais próximo.

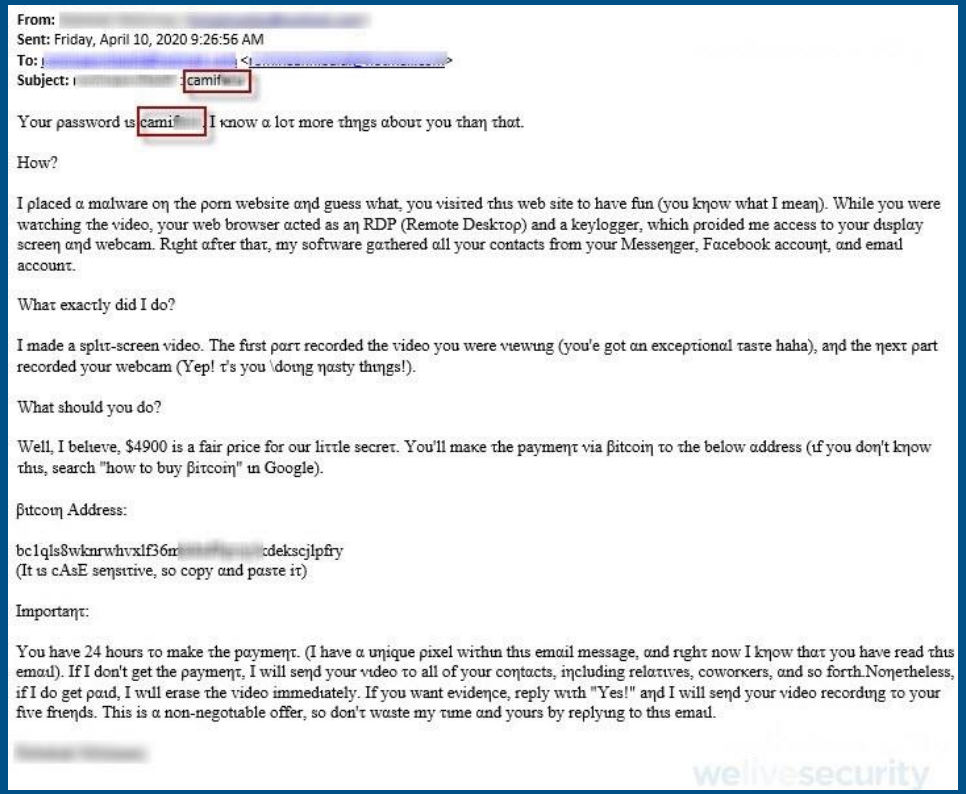
Está mensagem foi gerada automaticamente pelo sistema da CTT Expresso, não responda a está mensagem. Para cancelar a inscrição, clique aqui

© 2015 CTT EXPRESSO

CTT Expresso No Items

Exemplos de Emails de Phising

IP Telecom



From: [redacted]
Sent: Friday, April 10, 2020 9:26:56 AM
To: [redacted]
Subject: [redacted] camif[redacted]

Your password is camif[redacted]. I know a lot more things about you than that.

How?

I placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as an RDP (Remote Desktop) and a keylogger, which proided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. The first part recorded the video you were viewing (you'e got an exceptional taste haha), and the next part recorded your webcam (Yep! it's you \doing nasty things!).

What should you do?

Well, I believe, $4900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy Bitcoin" in Google).

Bitcoin Address:

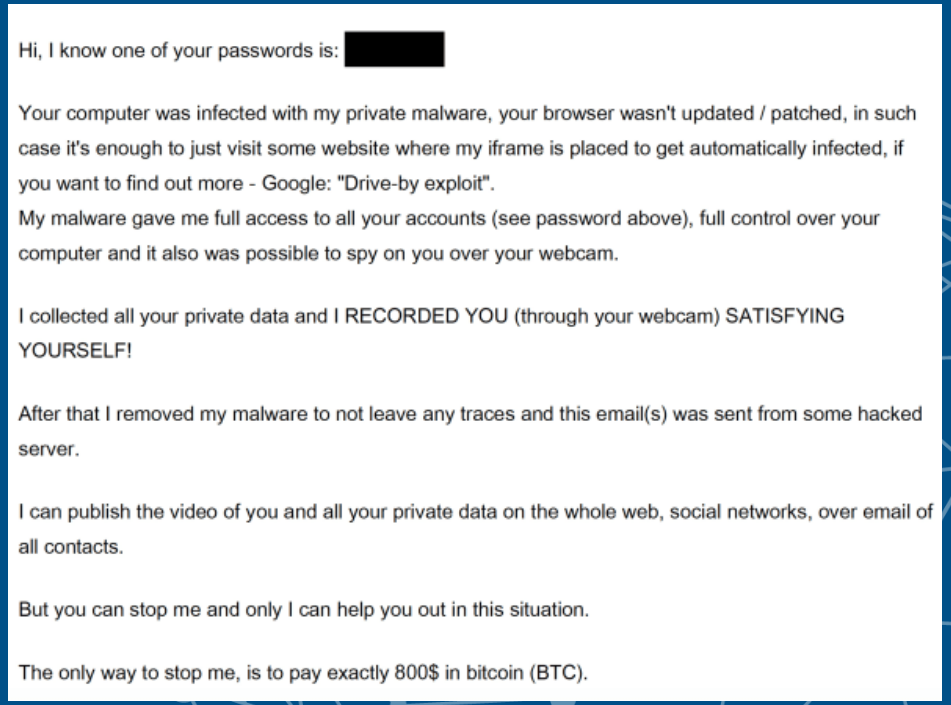
bc1qls8wknrwhvxlf36m[redacted]cdekscjlpfry
(It is cAsE sensitive, so copy and paste it)

Important:

You have 24 hours to make the payment. (I have a unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts, including relatives, coworkers, and so forth.Nonetheless, if I do get paid, I will erase the video immediately. If you want evidence, reply with "Yes!" and I will send your video recording to your five friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

[redacted]

welivesecurity



Hi, I know one of your passwords is: [redacted]

Your computer was infected with my private malware, your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".
My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spy on you over your webcam.

I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces and this email(s) was sent from some hacked server.

I can publish the video of you and all your private data on the whole web, social networks, over email of all contacts.

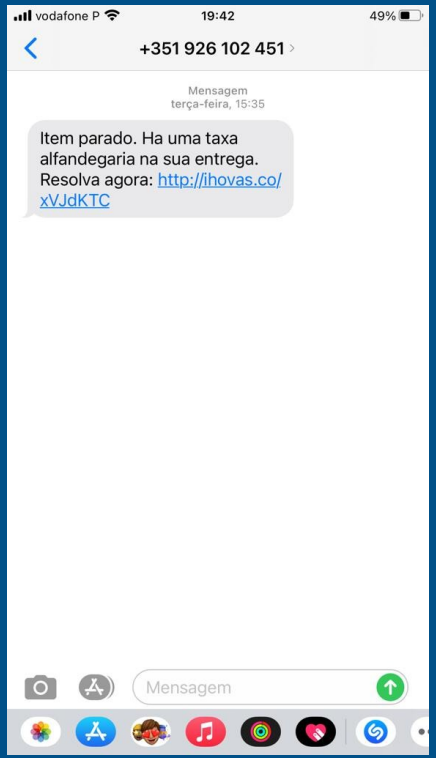
But you can stop me and only I can help you out in this situation.

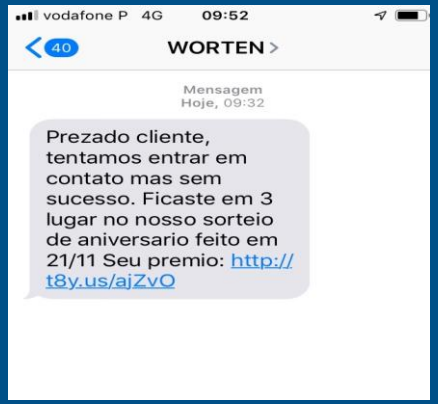
The only way to stop me, is to pay exactly 800$ in bitcoin (BTC).

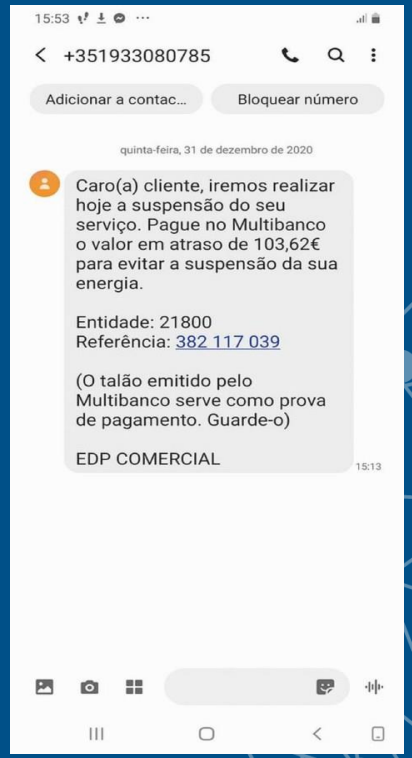
Outros tipos de “Phishing”

Smishing - Vishing

IP Telecom







"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012

Obrigado!

- @jose.sgoncalves
- @pedro.magalhaes

IP Telecom
Ligamos Negócios

cloudsolutions

IP Telecom

Ciclo sessões de cibersegurança

- **Análise de Emails – 29 de Março;**
- **Deteção de Malware – 13 de Abril;**
- **Gestores de Passwords - 26 de Abril;**
- **Melhores práticas a Respostas a Incidente – 10 de Maio;**
- **Engenharia Social – 24 de Maio.**

IP Telecom

Ligamos Negócios

www.iptelecom.pt

IP Telecom Portugal

/company/ip-telecom-portugal/