From awareness to culture:
Building an effective security program

Chester Wisniewski
Principal Research Scientist
October 2016
Who am I?
The problem
Which is easier to circumvent?
The keys to social engineering
I’m here to help
Criminal tactics
We’re good at detecting this

From: Agricultural Development Bank <agricultural@financier.com>
To: Undisclosed recipients
Subject: FW: Re Official
Security: GPG signed

Hello

MR George asked me to Forward you this email to Let you know we waited to hear back from you, please confirm if you are now ready to receive your approved $650,000 USD, LET US KNOW, so that we can re-invest it in our capital market.

George Kingsby (Investment banker)

Regards

Agricultural Development Bank.

Email: agricultural@financier.com
Not so good at this

From: Wells Fargo <info@wellsfargo.com>
To: chet.wisniewski@sophos.com
Subject: Wells Fargo Account Update - Important Message
Date: Tue, 26 Apr 2016 03:15:04 -0500 (CDT)

Hi chet.wisniewski@sophos.com,

You are kindly requested to confirm your Profile Details.

To confirm your details Continue and Sign on:

Continue and SignOn

Thank you for choosing Apple

Sincerely,
The Apple Team

We’re here to help. If you have any questions, just hit reply to this email and we’ll take care of the rest.

If you have any comments, suggestions or concerns regarding this email, please contact us. We respect your online time and privacy. This is an automated message. Please do not reply to this email.

You have received this email because you have agreed to have your Website Services Agreement and other service-affecting messages sent to you by email. NOTICE: This confidential email message is only for the intended recipient. If you are not the intended recipient, we advise that downloading, copying, distributing, or any other use of this message, is strictly prohibited. In such cases, please destroy this message and notify the sender.

Client Support

Our Banking is covered by our Online Security Guarantee. Learn more.

Our Site is covered by our Online Security Guarantee. Learn more.

Apple ID

Manage your Apple account

Your account
for everything Apple

Unsure of your Apple ID and password?

Remember me

Get Help with your Apple ID and password

Sign in with your Apple ID and password
Not so good at this
Dear Stephen,

Regarding the amount due 1572.98 GBP, we act on behalf of Cranfield Aerospace Ltd in order to collect the outstanding account value of your debt.

We would like to remind you that the amount above was due for payment on 29.03.16 but as no payment has been received, your invoice is now considered as overdue. Please find http://eduroute.ac-rouen.fr/index.php?q=evento-cv16yhalu-167dpsijipex-xc

Original invoice will be sent out to:

Stephen Fields
Loughton, Essex

In order to avoid further costs, please forward the payment to us and transfer the amount due not later than 12.04.16

Sincerely,

Todd Parks

---

Dear James,

Regarding the amount due 847.93 GBP, we act on behalf of Green Oaks Ltd in order to collect the outstanding account value of your debt.

We would like to remind you that the amount above was due for payment on 26.03.16 but as no payment has been received, your invoice is now considered as overdue. Please find http://ringwoodgrantwriters.com/index.php?axesi=5e8a1791c772216guros-wj

Original invoice will be sent out to:

James Road
Christchurch, Dorset

In order to avoid further costs, please forward the payment to us and transfer the amount due not later than 10.04.16

Yours truly,

Joseph Dawson
Open Source Intelligence

[Logos: Data.com Connect, Google, LinkedIn, Facebook]
Education only goes so far
What to do about it
The number is 3.
People
Creating a security culture
The great phish debate
Use the force

Always
Click

Suspicious

Report to IT

Figure 9.
Breach discovery methods over time,
(n=6,133).

Process
Assess risk
Focus where it matters most
Continuous improvement

- Set & Enforce Policy
- Prevent malware and hacking
- Monitor for compromises
- Respond to incidents
Continuous improvement
Compatible → cooperating

Integration within products:
- Firewall
- Web Filtering
- Download Reputation
- App Control
- Threat Engine
- Runtime Protection
- APT Detection

Integration across products:
- Next-Gen Firewall
- APT Detection
- MDM/EMM
- Encryption
- Antivirus
- Web Filtering
- Whitelisting

Sophos Central

SophosLabs

Next-Gen Enduser Protection
Next-Gen Network Security
Here to help

Sophos Home for PCs and Macs

SOPHOS
Security made simple.