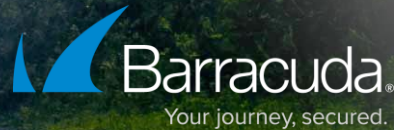
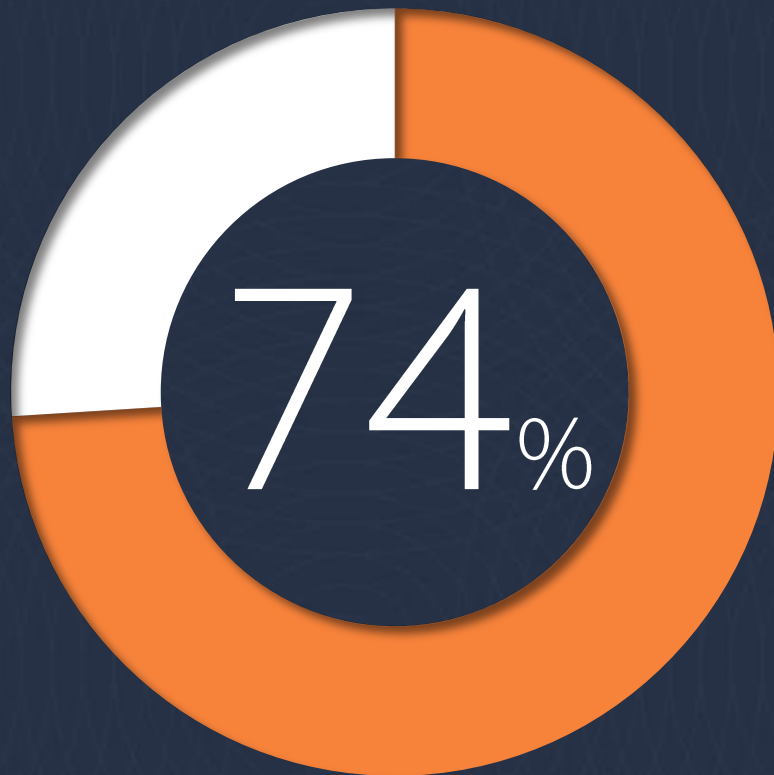


Total Email Protection

Comprehensive Email Protection—Made Radically Easy

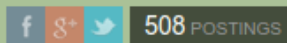


Targeted Attacks Start with Email



Neue Welle an Erpresser-Mails: "Habe dich beim Pornoschauen gefilmt"

18. Jänner 2019, 13:05




Behauptung ist zwar unbegründet, Betrugsversuch zeigt aber Gefahren von Passwort-Recycling

E-MAIL-SCAM

Save The Children verliert 1 Million US-Dollar an Betrüger

[Hacker](#) verschafften sich Zugriff auf das E-Mail-Postfach eines Angestellten der Kinderhilfsorganisation und legten dessen Kollegen mit gefälschten Zahlungsanweisungen herein. Dabei sind sie nicht alleine.

14. Dezember 2018, 11:36 Uhr, Jan Weisensee

 Alert! 16.01.2019 14:22 Uhr | Security

Erste Dynamit-Phishing Welle des Jahres: Trojaner GandCrab ist zurück

Unbekannte verschicken momentan massenweise gefälschte Bewerbungen, in denen ein Verschlüsselungstrojaner lauert.

MODLISHKA

Phishing-Tool umgeht Zwei-Faktor-Authentifizierung

Eine täuschend echte [Phishing](#)-Seite, die sogar [Zwei-Faktor-Authentifizierung](#) umgehen kann? Mit dem Tool Modlishka lassen sich automatisierte Phishing-Kampagnen betreiben - auch von sogenannten Scriptkiddies.

11. Januar 2019, 14:02 Uhr, Moritz Tremmel

Warnung vor Phishing-Mails mit Adresse help@orf.at

Seit einigen Stunden sind Phishing-Mails in Umlauf, die als Reply-Adresse help@orf.at eingetragen haben. Sie stammen nicht von der Ö1-Konsumentenredaktion und sollten nicht geöffnet werden.



Confidential

Barracuda Security Insight

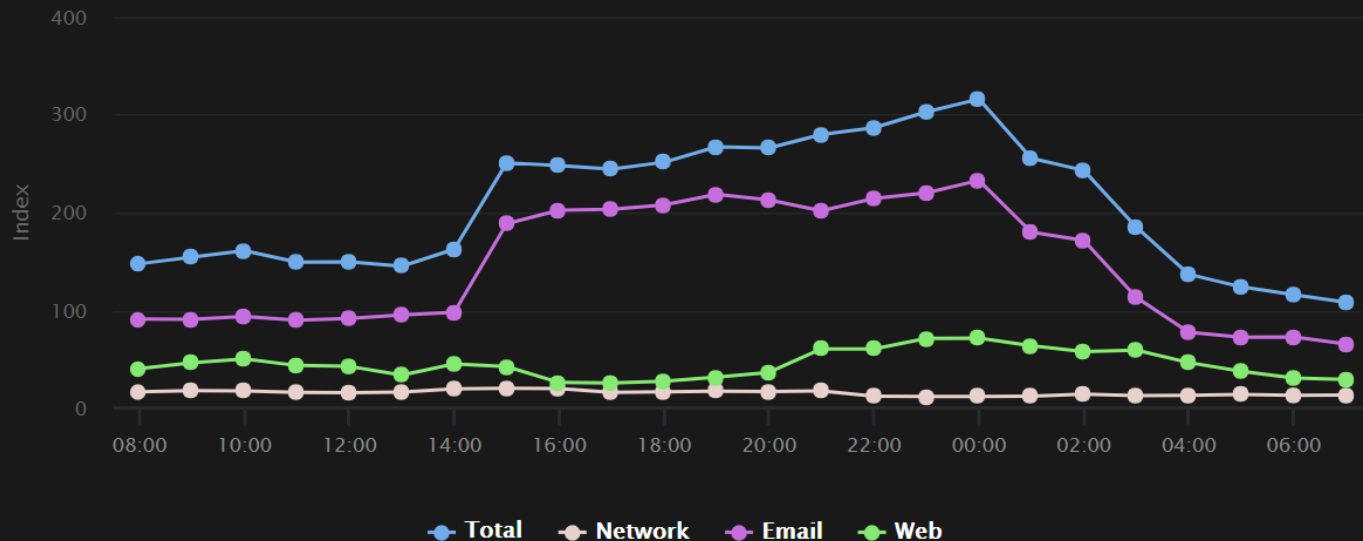
Current Threat Level: **Medium**

Current Cybersecurity Index: **108** ▼ 39.1

24 Hours

Previous 7 Days

Previous 30 Days



Zero-hour advanced threats in
last 24 hours

Total: **280,528**

Email: **263,987**

Web: **4,269**

Network: **12,272**



Barracuda Security Insight

Critical Alerts

Email Phishing via PDF

Affects: All OSes

Phishing PDFs have been observed as email attachments in phishing emails claiming to be DHL receipts. The PDF contains a bit.ly link to a spoofed Office365 sign in page.

[Read More](#)

LokiBot via Fake DOC

Affects: Windows

Malicious RTF files masquerading as Word documents have been observed as email attachments in phishing emails claiming to be purchase orders. The spreadsheet downloads

[Read More](#)

LokiBot via Fake Z

Affects: Windows

Email with attached ACE files with .z file extensions have been observed on emails claiming to be requests for quotation. The archive contains a LokiBot variant that

[Read More](#)

LokiBot via Fake r00

Affects: Windows

Email with attached RAR files with .r00 file extensions have been observed on emails claiming to be sales contracts. The archive

Pony via Fake ARJ

Affects: Windows

Email with attached ZIP files with .arj file extensions have been observed as email attachments claiming to be requests for

TrickBot via DOC

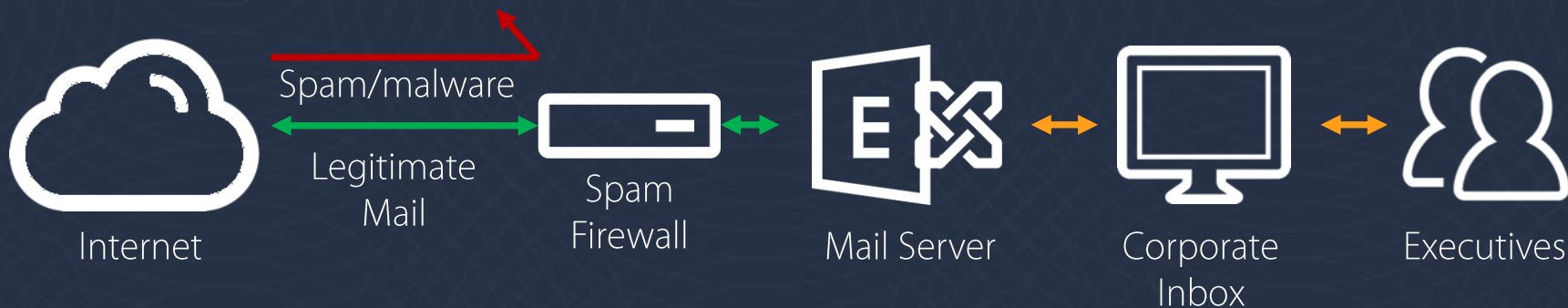
Affects: Windows

Malicious Word documents have been observed as email attachments in phishing emails claiming to be from CitiBank. The

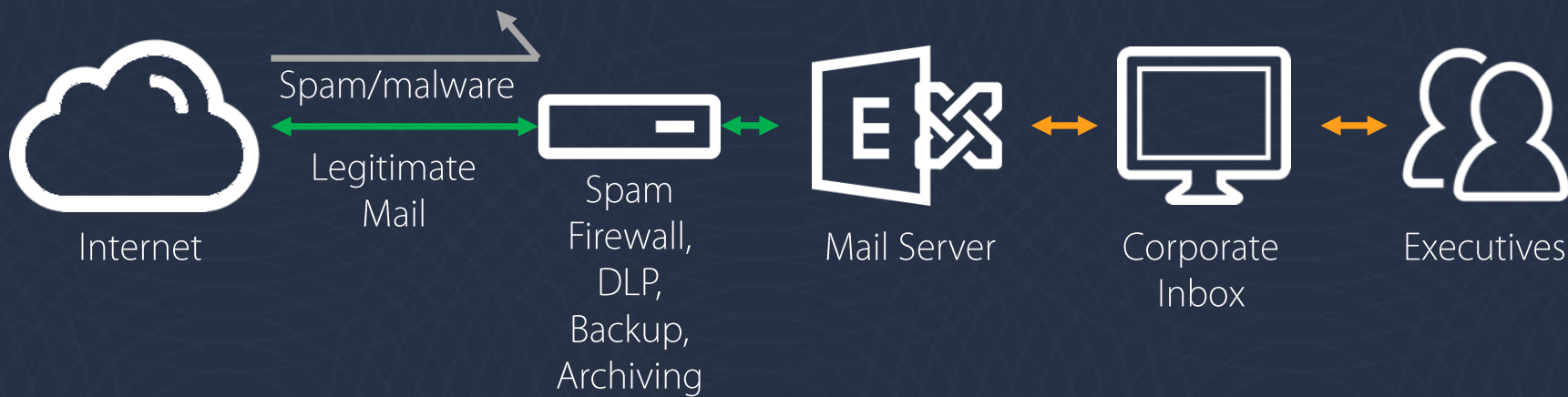
In the early days, it was simple



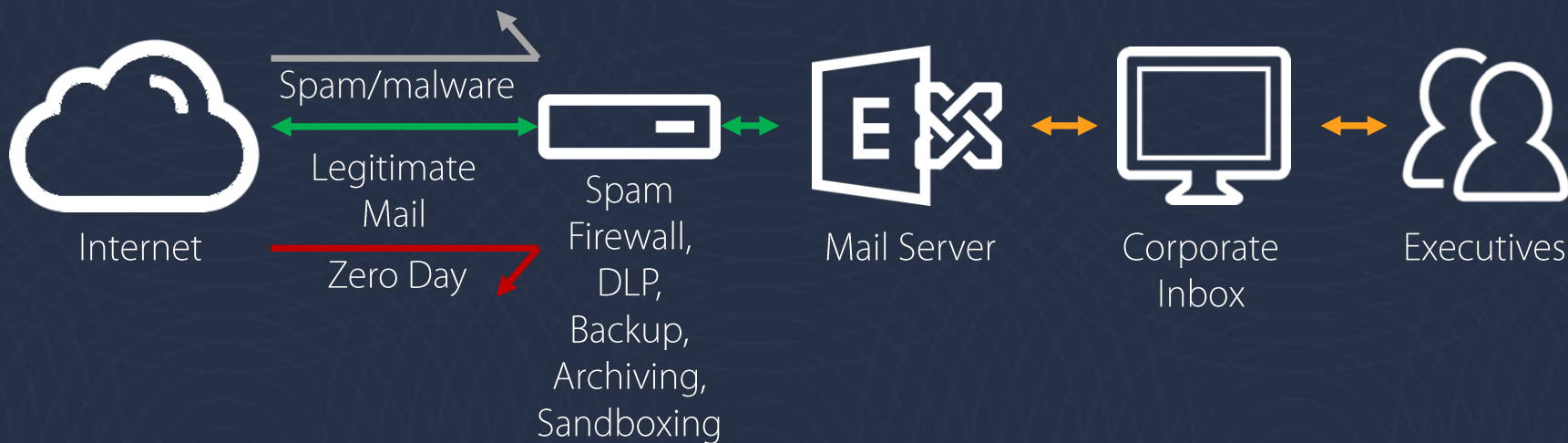
Spam firewalls kept bad things out



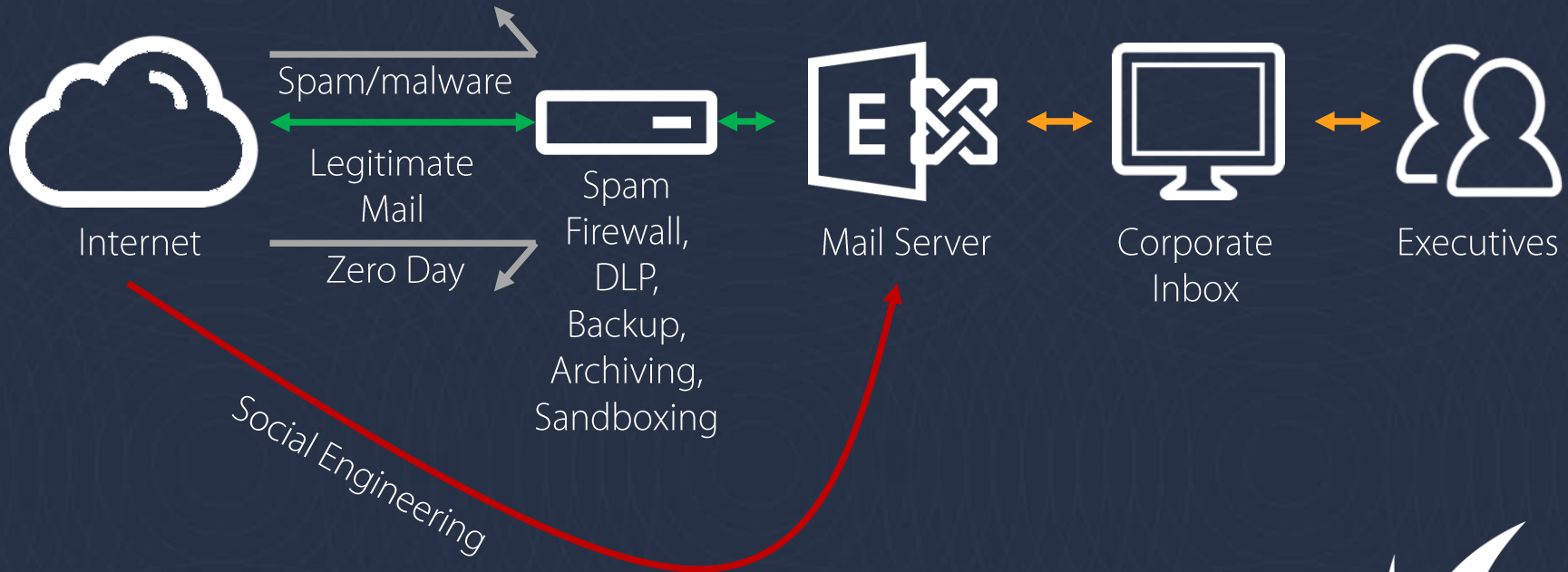
Over time, we built a better gateway



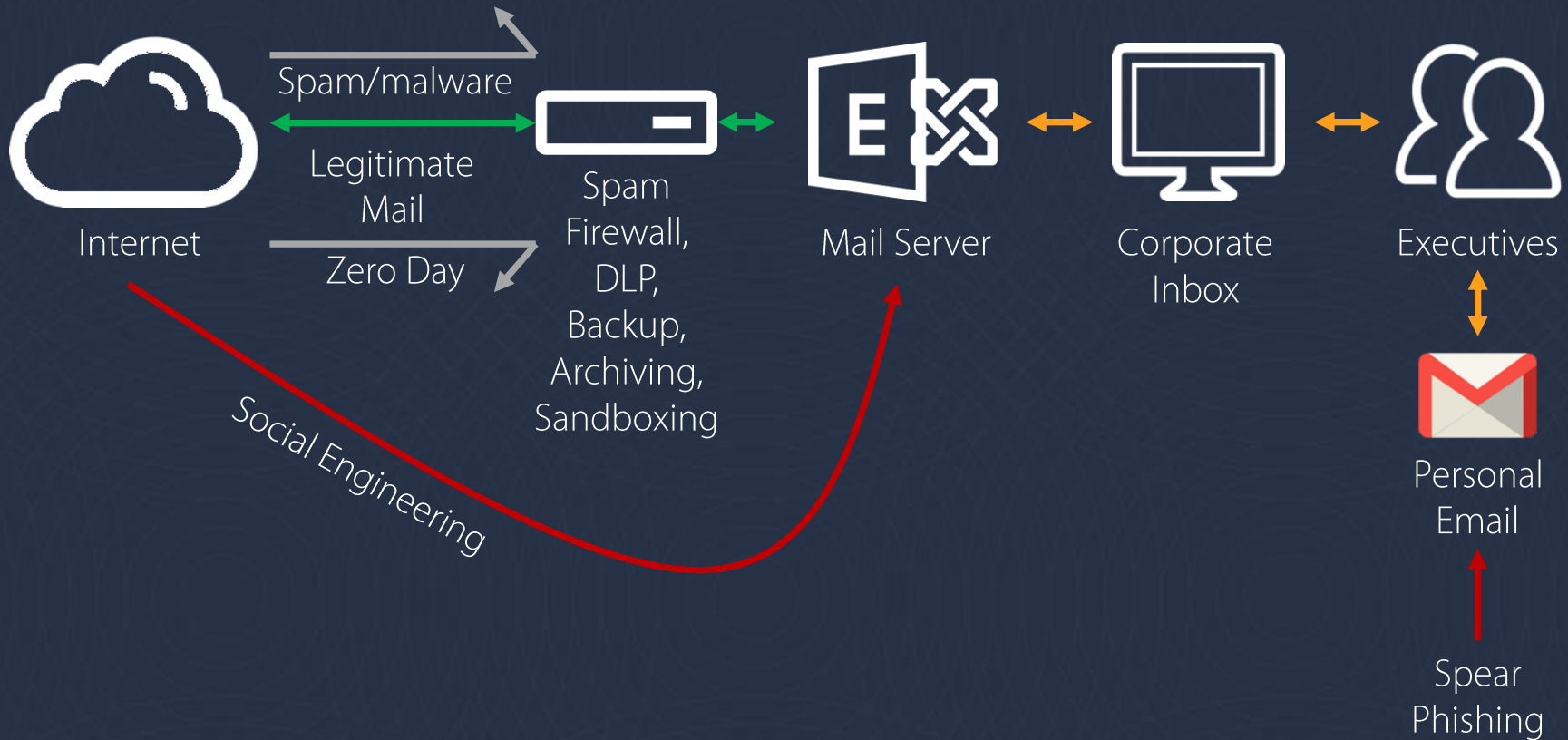
Sandboxing stopped zero day threats



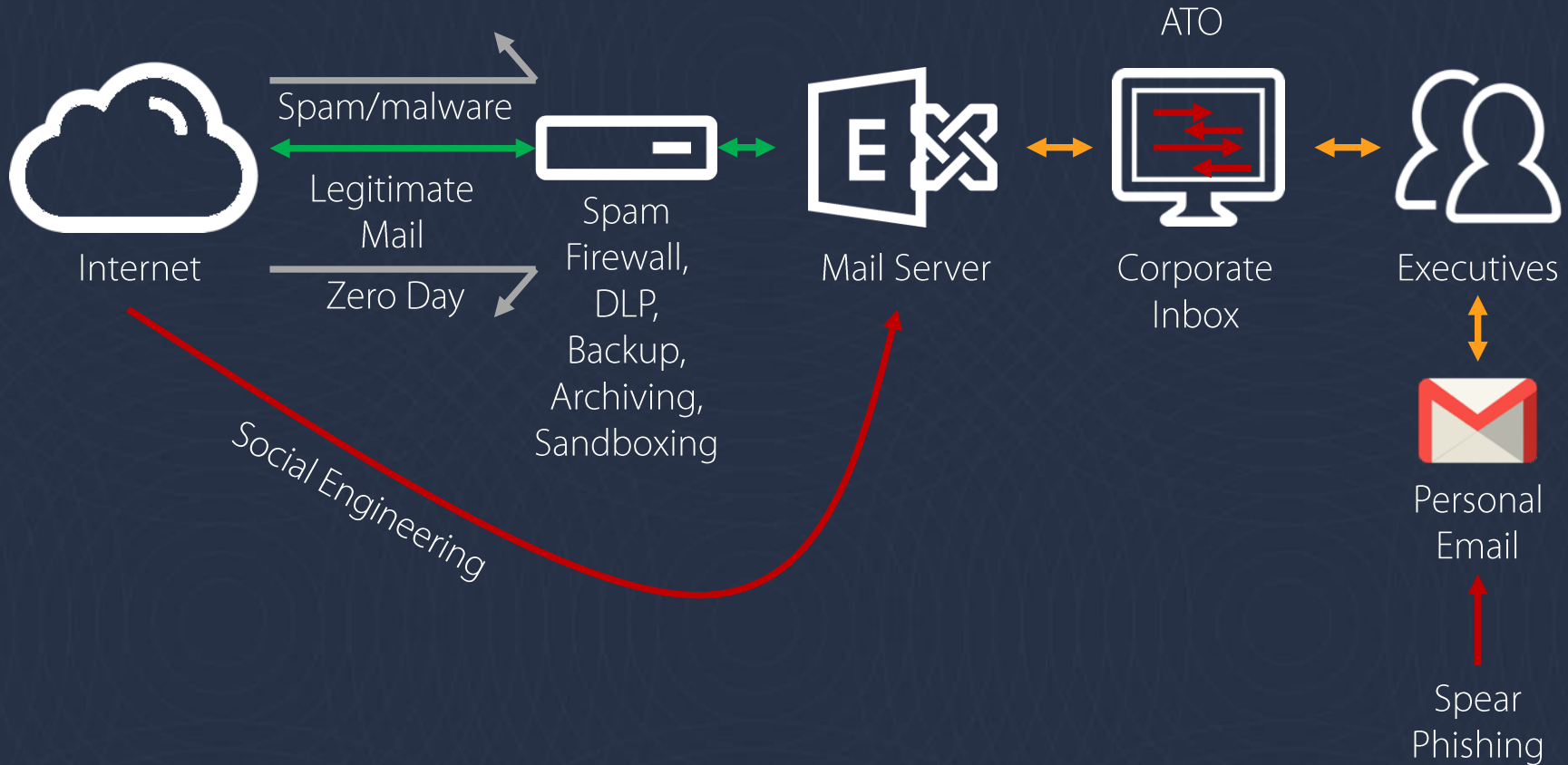
But gateways are blind to social engineering



And attacks are coming in through the back door



Account takeover is the newest threat



Securing the gateway is still **necessary**, but
no longer sufficient



Total Email Protection

ESS Barracuda **Essentials**

Make email safe for business with award-winning email-filtering, spam blocking, encryption, archiving, and backup.

SEN Barracuda **Sentinel**

Protects users and data from targeted spear phishing attacks and account takeover with an A.I. engine that detects threats that traditional email gateways cannot.

PL Barracuda **PhishLine**

Complete training and spear phishing simulation platform that empowers users to recognize email threats not only at work but also from devices that are not protected by corporate email gateways.

Barracuda Forensics and Incident Response

Automated incident response provides remediation options to quickly and efficiently address attacks.



Total Email Protection

ESS

**Barracuda
Essentials**

Make email safe for business with award-winning email-filtering, spam blocking, encryption, archiving, and backup.

SEN

**Barracuda
Sentinel**

Protects users and data from targeted spear phishing attacks and account takeover with an A.I. engine that detects threats that traditional email gateways cannot.

PL

**Barracuda
PhishLine**

Complete training and spear phishing simulation platform that empowers users to recognize email threats not only at work but also from devices that are not protected by corporate email gateways.

Barracuda Forensics and Incident Response

Automated incident response provides remediation options to quickly and efficiently address attacks.



Barracuda Essentials

Comprehensive security, archiving, and backup solution



- Office 365, on-premises and hybrid
- Simple quoting/bundling
- Per user licensing
- Web-based management

Advanced Email Security

Easy-to-Use, Cloud-Based Email Security



- Inbound Scanning
 - Spam filtering
 - Virus scanning
 - Malware scanning
 - Link protection
 - URL protection against typosquatting
 - DMARC enforcement

Advanced Email Security

Easy-to-Use, Cloud-Based Email Security



- Outbound Scanning
 - Spam filtering
 - Virus scanning
 - Malware scanning
 - DLP (Data Loss Prevention)

Advanced Email Security

Easy-to-Use, Cloud-Based Email Security



- Email Continuity
- Denial-of-Service prevention
- Secure Messaging (Encryption)

Prevent Advanced Threats

Barracuda Advanced Threat Protection



- Mehrschichtiges Verfahren
- Optimiert auf Geschwindigkeit und Effizienz
- Globales Threat-Intelligence Network

Global Threat Intelligence Network

All Threat Vectors



Network



Email



Web



Mobile Users



Application

Honey Pots

Crawlers

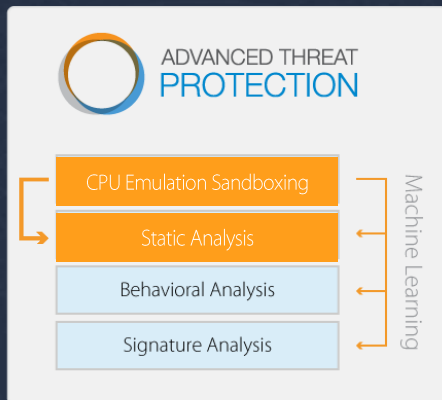
240,000
Deployments

Customer
Submissions

Barracuda Labs

Threat
Intelligence

All Advanced Threats



Barracuda Security Solutions



Barracuda
Essentials

ESG

Barracuda Email
Security Gateway

WSG

Barracuda Web
Security Gateway

NG

Barracuda
NextGen Firewall

WAF

Barracuda Web
Application Firewall



Total Email Protection

ESS Barracuda **Essentials**

Make email safe for business with award-winning email-filtering, spam blocking, encryption, archiving, and backup.

SEN Barracuda **Sentinel**

Protects users and data from targeted spear phishing attacks and account takeover with an A.I. engine that detects threats that traditional email gateways cannot.

PL Barracuda **PhishLine**

Complete training and spear phishing simulation platform that empowers users to recognize email threats not only at work but also from devices that are not protected by corporate email gateways.

Barracuda Forensics and Incident Response

Automated incident response provides remediation options to quickly and efficiently address attacks.



Conventional Email Gateway Security



Social Engineering is not stopped



Social Engineering is not stopped



Spear Phishing: Growing Exponentially

\$12B

Total Losses from spear phishing

FBI

1,100%

Increase from 2015-2017

FBI



Comprehensive Defence



AI for
Real-Time
Spear
Phishing
Prevention



Domain
Fraud
Visibility and
Protection
with DMARC



Account
Takeover
detection
and
remediation



Phishing Attacks

Trick users into doing something wrong

- Transferring money to the attacker
- Giving away their account logon – Account Takeover
- Giving away sensible information

Many ways to do this

- Web Service impersonation
- Employee impersonation – building trust



From:

Microsoft Outlook

Subject: Action required

Microsoft office365 Account

Review recent activity

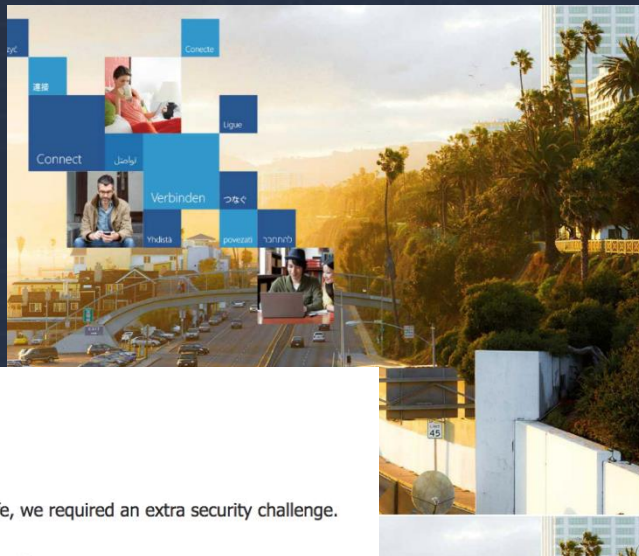
We detected some unusual activities on your Microsoft office365 Account. To help keep you safe, we required an extra security challenge.

And to avoid deactivation, Please review your recent activity and we'll help you take corrective action.

[Review recent activity](#)

To opt out or change where you receive security notifications, [click here](#).

Thanks,
The Microsoft account team



Office 365

Work or school, or personal Microsoft account

Email or phone

Password

☐ Keep me signed in

[Sign in](#)

[Back](#)

[Can't access your account?](#)

© 2017 Microsoft
[Terms of use](#) [Privacy & Cookies](#)

Microsoft

Office 365





Microsoft

Microsoft Office365 Email Account Expires In 48 Hours

Your Microsoft Office 365 email account will expire in 48 hours reactivate by clicking on the reactivation button below.

[Re-Activate](#)

If you choose not to reactivate your email data will be deleted without further notice. Any additional active subscriptions you might have will not be affected by this deletion.

Subscription information:

Subscription ID: 1b0bec96-3435-4ftb-b632-cc7da174c7e6

Helpful resources

[How to reactivate your Office 365 subscription](#)

[What happens to my data and access when my subscription expires?](#)

[Get help and support for Office 365](#)

This is a mandatory service communication. To set your contact preferences for other communications, [click here](#).

This message was sent from an unmonitored e-mail address. Please do not reply to this message.

[Privacy](#) | [Legal](#)

Microsoft Office
One Microsoft Way
Redmond, WA
98052-6399 USA





28.09.2013

Sehr geehrter Kunde,

Im Rahmen unserer Sicherheitsmaßnahmen prüfen wir regelmäßig alle Vorgänge im PayPal-System. Bei einer Überprüfung haben wir kürzlich ein Problem im Zusammenhang mit Ihrem Konto festgestellt.

Zu Ihrem Schutz haben wir den Zugriff auf Ihr Konto eingeschränkt, bis zusätzliche Sicherheitsmaßnahmen getroffen werden können. Wir bitten um Entschuldigung für eventuelle Unannehmlichkeiten.

Was mache ich jetzt ?

Bitte verifizieren Sie sich über folgenden Link durch einen Abgleich Ihrer Daten als rechtmäßiger Besitzer. Im Anschluss können Sie Ihr Konto wieder uneingeschränkt nutzen.

[hier klicken](#)

Mit freundlichen Grüßen

Ihr PayPal-Team

Why Sentinel?

Spear Phishing wird von Gateway-Lösungen nicht gestoppt:

- Keine böartigen Anhänge oder Links
- Kleineres Volumen und personalisierte Angriffe



REPORT MISSED ATTACK

TEST AI



RECENT ATTACKS

REPORTS

PROTECTION STATUS FOR BARRACUDA

7 mailboxes protected

0 quarantined spear phishing attacks

Mar 30, 2018
7:18 PM last email processed

SPEAR PHISHING ATTACKS

Emails in your account that have been identified as fraud attempts.

FILTER ATTACKS

EXPORT TO CSV

Search

Date ▾

Employee

Email

Status

No emails

Page: 1 ▾ 0 - 0 of 0 < >



Absender Authentifizierung

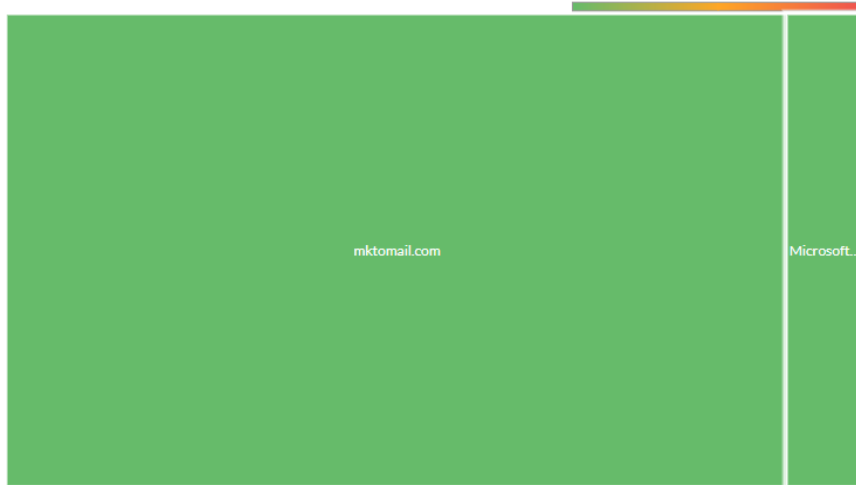
- Domain Fraud Protection:
 - liefert Transparenz und Analyse von DMARC-Berichten, die Phishing und Brand Hijacking verhindern und die Zustellbarkeit des legitimen E-Mail-Verkehrs sicherstellen.



HIGH VOLUME SENDERS

Services that are sending a high volume of emails from your domain

EXPORT TO CSV



Hover for more information, click to drill down

GEOGRAPHIES

Where emails from your domain are coming from



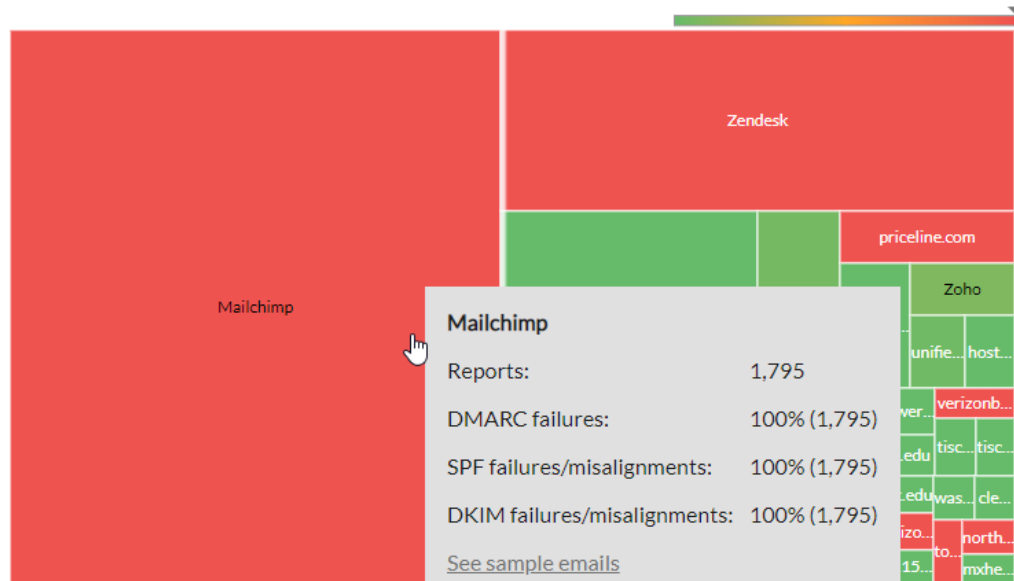
Larger markers stand for higher total volume, redder markers stand for higher volume from blacklisted IPs



OTHER SENDERS

Services that are sending a lower volume of emails, potentially fraudulent

EXPORT TO CSV



Mailchimp

Reports: 1,795

DMARC failures: 100% (1,795)

SPF failures/misalignments: 100% (1,795)

DKIM failures/misalignments: 100% (1,795)

[See sample emails](#)

[SPF setup instructions](#)

[DKIM setup instructions](#)

[Go to mailchimp.com](#)

Hover for more information, click to drill down



Account Takeover

Angreifer bekommt Zugriff auf einen Account

- Ausspähung
- Angriffe intern
- Angriffe nach extern

Key insight:

- Sentinel arbeitet mit Kommunikationshistorie um solche Angriffe zu korrigieren



ALERTS BETA


Account takeover incidents detected by Sentinel's AI

Date

No alerts

INCIDENTS

Account takeover Incidents previous

 EXPORT TO CSV

1 ▾ 0 - 0 of 0 < >

NEW INCIDENT

New account takeover incident

1 2 3 4 5 6 7

Here's what we are going to do

1. **Internal clean up:** remove malicious emails from your users' mailboxes to prevent further takeovers.
2. **External notification:** mitigate reputation and brand risk by letting external parties know they received a malicious email from you.
3. **Block access:** prevent further use of the compromised account by the attacker.

CANCEL

NEXT



Email Threat Scanner

BARRACUDA NETWORKS'S SCAN FROM JUN 05, 2017



0

Fraudulent emails



3

Employees at risk



2

Domain fraud risks



14

Mailboxes

SPEAR PHISHING AND FRAUD

 FILTER ATTACKS

 EXPORT TO CSV

 Search

Last received ▾

Times received

Employee

Email

No attacks

Page: 1 ▾ 0 - 0 of 0 < >

DOMAIN RISK

2 domains at spoofing and fraud risk

[Recommendation](#)



scan.barracudanetworks.com
can be spoofed and used for fraud



sookasa.co
can be spoofed and used for fraud



Kreieren Sie Ihren persönlichen Link:

<https://scan.barracudanetworks.com/mylink>

Lassen Sie Ihre Kunden den Threat Scan ausführen (kann 1-2 Tage dauern)

Besprechen Sie das Ergebnis

Lassen Sie von einem SE Ihrer Region den Report in eine DEMO Produktivumgebung umwandeln (30 Tage)

GET YOUR PERSONALIZED LINK

1. Enter your email

Email *

2. Copy this personal Email Threat Scanner sign up link



3. Share this link with all your Office 365 customers to help them scan their accounts for advanced threats.

To track scans from your personalized link, visit [How many scans?](#)



**Barracuda
Email Threat Scanner**

Barracuda Email Threat Scanner is a tool that can help you sell more. Your customers can scan their Office 365 accounts and get a personalized report on advanced threats that are already in their account. Signing up for a scan takes 2 minutes and it's 100% free.

Customers that scanned their accounts found 10s or 100s of threats, and signed up for Barracuda Email Security in a snap. [Watch our training webinar.](#)



Total Email Protection

ESS

**Barracuda
Essentials**

Make email safe for business with award-winning email-filtering, spam blocking, encryption, archiving, and backup.

SEN

**Barracuda
Sentinel**

Protects users and data from targeted spear phishing attacks and account takeover with an A.I. engine that detects threats that traditional email gateways cannot.

PL

**Barracuda
PhishLine**

Complete training and spear phishing simulation platform that empowers users to recognize email threats not only at work but also from devices that are not protected by corporate email gateways.

Barracuda Forensics and Incident Response

Automated incident response provides remediation options to quickly and efficiently address attacks.

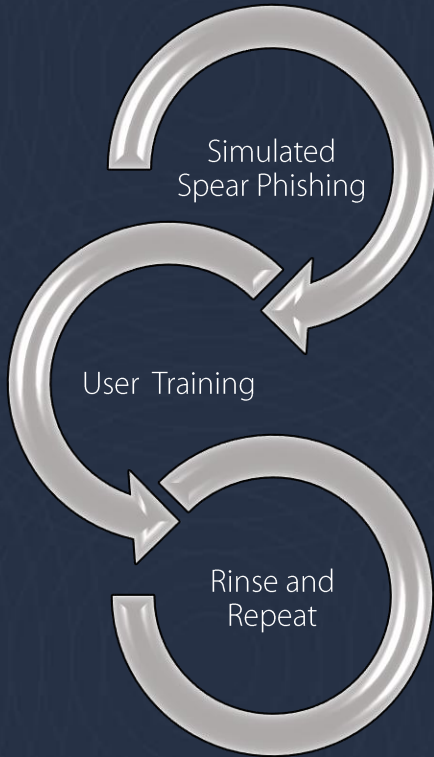


What does PhishLine do?

Simuliert Phishing Angriffe und testet, sowie trainiert, Mitarbeiter auf ihre Fähigkeit gefälschte Emails und andere Phishing (smishing Versuche zu erkennen.



User Education – Der Trainingszyklus



Spear Phishing Simulation zur Auswertung der Mitarbeiter

- Mehrere parallele "hooks"
- Verschiedenste Landing Pages





(email:firstName) (email:lastName)



You have a new connection request



Sarah Jesswin

Senior Recruiter - Hexton Placement Agency

[Accept Request](#)

[View Profile](#)

What else is going on in your network?



Joe Kelly got a new job as senior email designer

[Say Congratulations](#) • [View Profile](#)



Kathryn May is celebrating 2 years at WestIvee

[Say Congratulations](#) • [View Profile](#)



Doug Blume is celebrating 5 years at Aaron Carter Elementary

[Say Congratulations](#) • [View Profile](#)

[Sign In To Your Account](#)

You are receiving LoopedNow Network Notifications. This email was intended for (email:firstName) (email:lastName).
If you need assistance or have questions, please contact LoopedNow Customer Service.
©2017, LoopedNow, 4029 Albanian Ct, CA 94042, USA

[Click Here To Unsubscribe](#)



Account Number: 934235235

Transaction ID: T7382I3Y9Q32

You Successfully Sent Money

From: (email:firstName) (email:lastName)

Amount: \$80.00

To: Larry Cooper

For: Technical Maintenance

Customer Service URL: www.cooptechnsolutions.com

To change or cancel your agreement with Larry Cooper, log in to your FinancialFriend account, go to your Profile, and click My Payments.

If you'd like to update your agreement, you can do so in the "Trusted Vendor" section of your account.

Sincerely,
FinancialFriend

[Helpful Resources](#) | [Security Portal](#)

Please do not reply to this email. To contact us, click [here](#). | ©2017 FinancialFriend. All rights reserved.

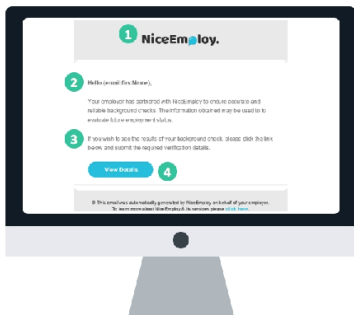


You've Been Phished!

This was a training exercise conducted by our Information Security Team.

Phishing is the #1 method attackers use to steal your personal and our company's information and gain access to our network.

Here are some tips to help keep you safe at home and at work:



1

Tip Text Here

2

Tip Text Here

3

Tip Text Here

4

Tip Text Here

Always report suspicious emails and events to phishing@companyname.com

[Training Link](#)

Access All Accounts

Sign in to continue

[Sign in with a different account](#)

Access All Accounts



User Education – Der Trainingszyklus



Mitarbeitertraining basierend der Reaktion auf die simulierten Angriffe.

- Angepasst an das Wissenslevel des Mitarbeiters. Kein Mitarbeiter sollte sofort mit den komplexesten Phishing Taktiken konfrontiert werden. (levelized training)
- Unterschiedliche Trainingsformate (gamification)



Animated Training Modules—Availability

PHISHING 101

P101A—1



Run Time
2:47

A high-level introduction to the concept of phishing.

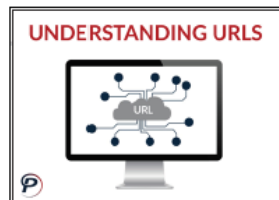
P101A—2



Run Time
2:58

An overview of phishing techniques, including phishing, spear phishing, smishing and vishing.

P101A—3



Run Time
4:56

Insights into web addresses that can protect users while browsing and working online.

P101A—4



Run Time
3:46

A look at some of the most popular phishing scams and how to prevent being victimized.

AWARENESS 101

A101A—1



Run Time
2:32

Tips on keeping company data secure and being alert to the methods of hackers.

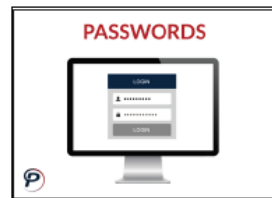
A101A—2



Run Time
2:21

Focuses on adhering to policies and procedures designed to safeguard company data.

A101A—3



Run Time
2:00

A look at what makes strong passwords strong, plus tips on creating the most effective ones.

A101A—4



Run Time
2:53

Steps one can take to protect mobile devices from being accessed by thieves and hackers.

A101A—5



Run Time
1:57

Outlines how to respond when faced with a suspicious phishing attempt.

A101A—6

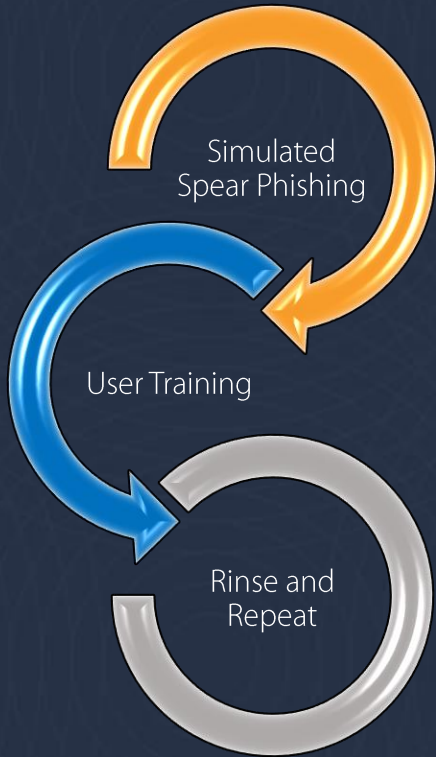


Run Time
1:26

Tips on avoiding being manipulated by scammers, hackers and social engineers.

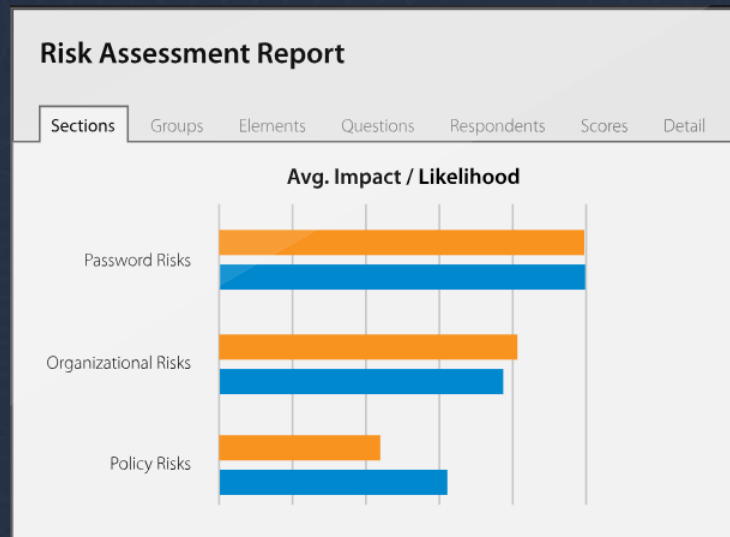
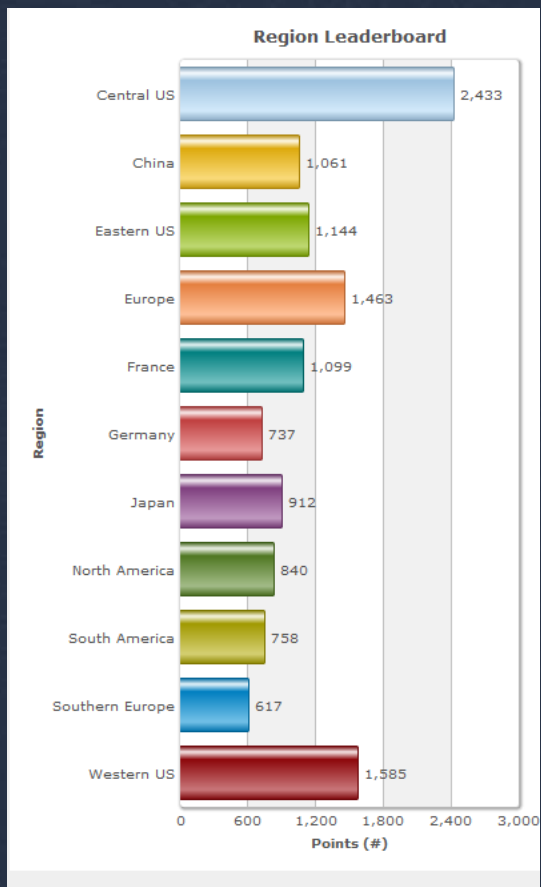


User Education – Der Trainingszyklus

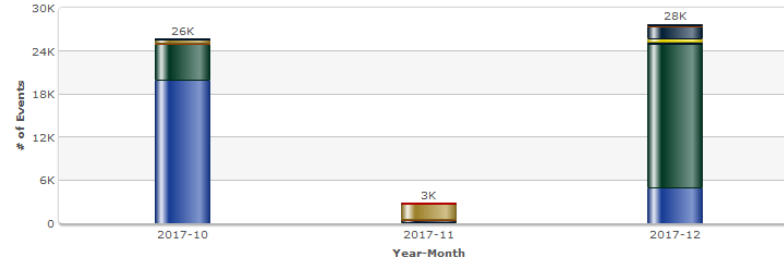


Detaillierte Auswertungen um Verbesserungen/Verschlechterungen aufzuzeigen.

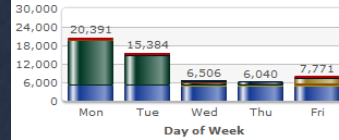




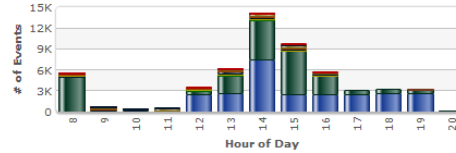
Event Count by Year-Month
Data displayed is for Time Zone: America/Chicago



Event Count by Day of Week
Data displayed is for Time Zone: America/Chicago



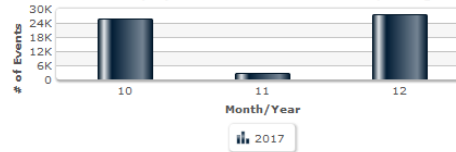
Event Count by Hour of Day
Data displayed is for Time Zone: America/Chicago



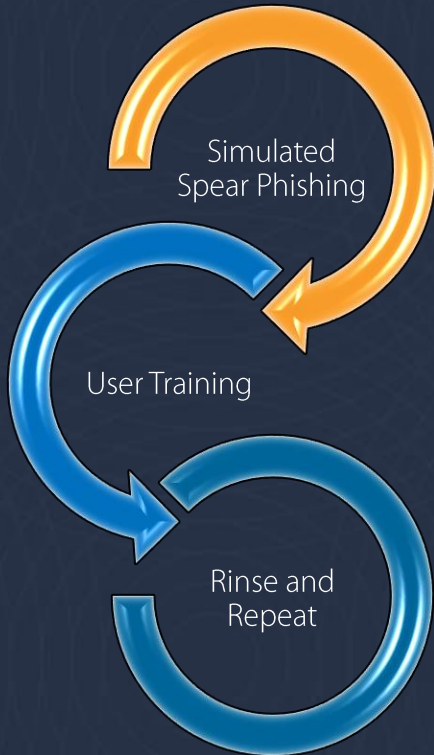
Event Count Quarterly Comparatives
Data displayed is for Time Zone: America/Chicago



Event Count Monthly Comparatives
Data displayed is for Time Zone: America/Chicago



User Education – Der Trainingszyklus



The cycle repeats for continuous improvement



Training der "Human Firewall"

Von einem einmaligen Workshop auf wiederholendes Training wechseln.

Security kann einfach in eine bestehende Organisationskultur integriert werden.

Der Schlüssel zum anti-phishing Erfolg ist das Engagement der Mitarbeiter



PhishLine Product Suite

- Barracuda PhishLine
 - Priced per user, 100 minimum
 - Customer customizes and runs programs
 - Barracuda Support
- Barracuda PhishLine Concierge
 - Fixed price
 - PhishLine consultant customizes and runs program
 - PhishLine consultant provides support



Total Email Protection

ESS Barracuda **Essentials**

Make email safe for business with award-winning email-filtering, spam blocking, encryption, archiving, and backup.

SEN Barracuda **Sentinel**

Protects users and data from targeted spear phishing attacks and account takeover with an A.I. engine that detects threats that traditional email gateways cannot.

PL Barracuda **PhishLine**

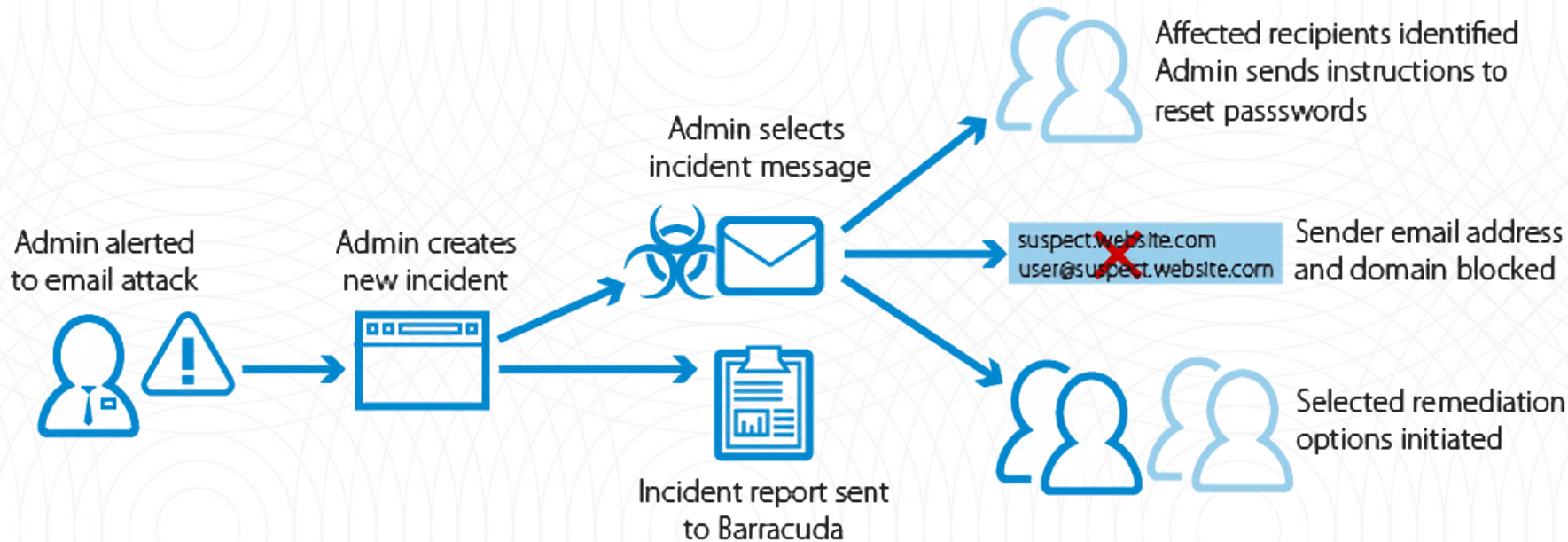
Complete training and spear phishing simulation platform that empowers users to recognize email threats not only at work but also from devices that are not protected by corporate email gateways.

Barracuda Forensics and Incident Response

Automated incident response provides remediation options to quickly and efficiently address attacks.



What is it about?



INCIDENTS

Forensic incidents previously reported.



DID A MALICIOUS EMAIL SNEAK THROUGH THE SPAM FILTER?

Click "New Incident" to investigate and remediate the attack

[NEW INCIDENT](#)

Created On

Incident

Number of Messages Received

No incidents

Page:

1 ▾

0 - 0 of 0



Thank You

