ISSA

Information Systems Security Association International

www.issa.org

ISSA Thought Leadership Webinar

2018 User Risk Report

December 12, 2018

2018 User Risk Report

Today's web conference is generously sponsored by:

Wombat Security

https://www.wombatsecurity.com/

2018 User Risk Report

Moderator

Michael Levin, CEO/Founder, Center for Information Security Awareness

Michael Levin is a nationally known cyber security professional who spent over twenty-two years in the U.S. Secret Service protecting Presidents and Heads of State. Michael retired from the U.S. Department of Homeland Security - as the Deputy Director of the National Cyber Security Division in Washington DC. He enjoyed a distinguished thirty-year career in public service and law enforcement.

After this distinguished career and seeing the need, Michael founded the Center for Information Security Awareness – www.CFISA.com The CFISA was created to explore ways to increase cyber security awareness among many audiences, including consumers, employees, businesses and law enforcement. CFISA provides online and on-site cyber security awareness training services to businesses and organizations of all sizes.

2018 User Risk Report

Speaker

Gretel Egan, Security Awareness and Training Strategist, Wombat Security

Gretel Egan is the Security Awareness and Training Strategist for Wombat Security, a division of Proofpoint. A graduate of Carnegie Mellon University, she has extensive experience in researching and developing cybersecurity education content and was named one of “10 Security Bloggers to Follow” by IDG Enterprise. Gretel has written and provided commentary for national, industry, and trade publications, and has previously presented at events hosted by SecureWorld, Infosecurity Europe, ISACA, SC Media, and others.

2018 User Risk Report

Speaker

Kelly Robertson, CEO, SEC Consult America

Kelly Robertson, CISSP, has been an information security practitioner for more than 25 years and is a member of the Silicon Valley chapter of ISSA.
Kelly is currently CEO of SEC Consult America, a full-service information security consultancy based in Santa Cruz, California.

Mr. Robertson is an evangelist for cybersecurity awareness, presenting frequently to audiences and corporate organizations. He develops training and education programs for practical risk awareness to benefit people both personally and professionally. Kelly is committed to the enablement of the civil rights for digital citizens to include information security and data privacy.

2018 User Risk Report

Speaker

Richard Bird, Chief Customer Information Officer, Ping Identity

Richard Bird is the chief customer information officer for Ping Identity. He has spent more than 20 years in corporate business, technology and roles within multiple industries. His diverse background includes serving as the CIO for one of the world's largest hedge fund administrators to being the CISO for a high-tech Swiss analytic device company. Richard's combination of IT operations and security have afforded him the opportunity to be recognized as an expert in identity-centric security, along with many other security domains such as threat and vulnerability management, as well as data and cloud security. An author and frequent speaker on a broad range of cybersecurity topics, Richard is widely recognized as an identity evangelist

2018 User Risk Report

Speaker

Gretel Egan, Security Awareness and Training Strategist, Wombat Security

Gretel Egan is the Security Awareness and Training Strategist for Wombat Security, a division of Proofpoint. A graduate of Carnegie Mellon University, she has extensive experience in researching and developing cybersecurity education content and was named one of “10 Security Bloggers to Follow” by IDG Enterprise. Gretel has written and provided commentary for national, industry, and trade publications, and has previously presented at events hosted by SecureWorld, Infosecurity Europe, ISACA, SC Media, and others.

End Users: The Red Thread

98% Phishing and pretexting represent 98% of all incidents and 93% of breaches featuring social engineering.[1]

95% Nearly all phishing attacks that led to a breach were followed by an installation of malware.[1]

93% More than 90% of data breaches in 2017 could have been prevented.[2]

90% 90% of employees admit to violating policies designed to prevent security incidents.[3]

1. 2018 Verizon Data Breach Investigations Report
2. 2018 OTA Cyber Incident & Breach Response Guide
3. CEB Executive Guidance: Managing the Hidden Causes of Data Breaches

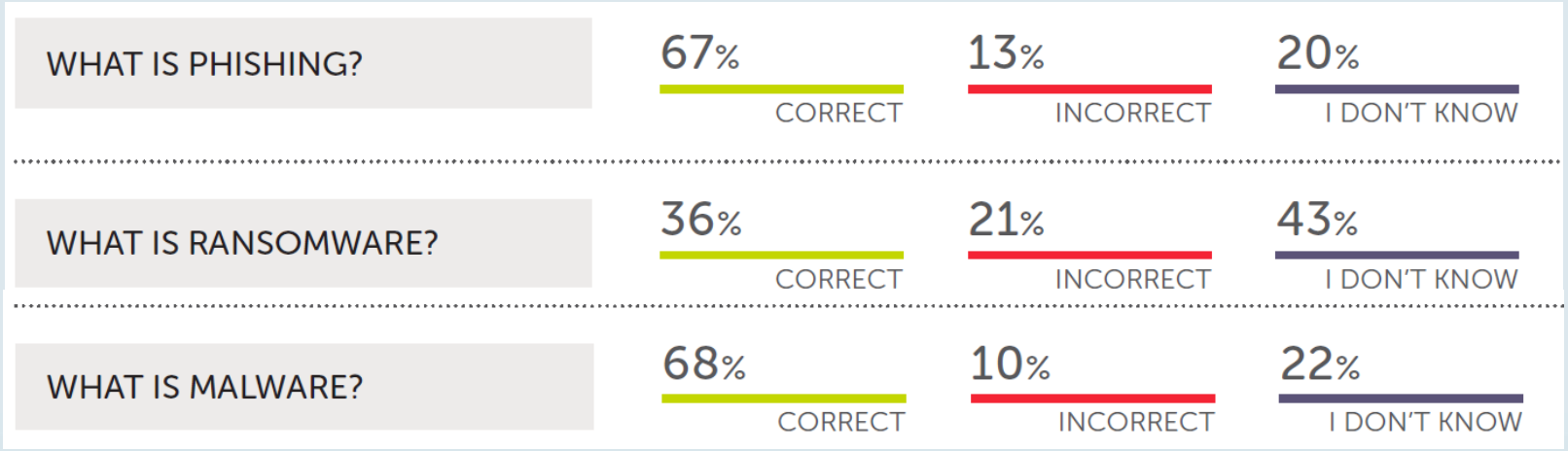
Cybersecurity Fundamentals

What does the average working adult know about security?

2018 User Risk Report

- Third-party survey of more than 6,000 working adults across six countries (US, UK, France, Germany, Italy, Australia)
- Questions about general cybersecurity topics and personal cybersecurity habits
- Results reflect global averages

Lack of Fundamental Cybersecurity Knowledge



Additional User Risk Report Findings

ISSA
Information Systems Security Association International

44%	of respondents **do not password-protect** their home WiFi networks
66%	have not changed the **default password** on their WiFi routers
14%	of users have **no security lock on their smartphones**
28%	are relying on a **four-digit PIN** to secure their smartphones
MORE THAN 60%	of respondents who don't use a password manager admit to **reusing passwords across online accounts**
55%	of working adults who use employer-issued devices at home **allow friends and family members** to access those devices

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

2018 User Risk Report

Speaker

Kelly Robertson, CEO, SEC Consult America

Kelly Robertson, CISSP, has been an information security practitioner for more than 25 years and is a member of the Silicon Valley chapter of ISSA.
Kelly is currently CEO of SEC Consult America, a full-service information security consultancy based in Santa Cruz, California.

Mr. Robertson is an evangelist for cybersecurity awareness, presenting frequently to audiences and corporate organizations. He develops training and education programs for practical risk awareness to benefit people both personally and professionally. Kelly is committed to the enablement of the civil rights for digital citizens to include information security and data privacy.

Click on the Dancing Pig!

"The applet DANCING PIGS

could contain malicious code that might do permanent damage to your computer, steal your life's savings, and impair your ability to have children."

Phishing: Remarkably Effective

- The Wide Net, the Spear Phish and the Web
  - Employees targeted as consumers
  - Business Email Compromise – Spoofing a trusted internal person
  - Visiting hostile websites – hundreds of thousands of new sites each month
- Previously industrial scale, increasingly spearing individuals and soft targets
- 95% of all attacks on Enterprise networks are the result of successful Spear phishing – SANS Institute
- 30% of phishing messages are opened by users, 12% of those users click through – Verizon DBIR
- 76% of businesses reported being a victim of a phishing attack in the last year – Wombat Security

Ransomware: Serious Consequences

- Malware that is attached to or embedded in email
- Encrypts the victim's file system
- Can spread to many other systems rapidly
- Attacks yield an average of $1,077 per
- Ransomware attacks fell nearly 30% over the past 12 months - Kaspersky
- Dropped from #1 malware payload in 2016 to #6
- Less than 5% of malware
- Difficult to monetize
- Anti-phishing techniques are effective

Anatomy of an effective Phish

From: Janet XXXX [mailto: mngt@XXXXmail.com]

Sent: Thursday, June 14, 2018 7:34 AM

To: ArleneXXXX@XXXX.org

Subject: Payment

Importance: High

Arlene,

Do you have a moment? We have a pending invoice from our Vendor.

I have asked them to email me a copy of the invoice, Can I send it to you for processing once I receive it?

Best regards,

Janet

Anatomy of an effective Phish

On 2018-06-14 16:27, Arlene wrote:

Yes, I received it. We will pay this invoice next Wednesday.

Thank you,

Arlene XXXX

Finance Director

XXX-XXX-XXXX

XXXX@XXXX.org

Anatomy of an effective Phish

The invoice appeared to be authentic:

From
P&A XXXXX
407 XXXX XXXX Drivew
XXXXX, SC 29XXX
United States of America

To
XXXX
Street Address
City, State Zip
United States of America

Invoice No.
INV-WC55232

Date
June 14, 2018

Invoice Due
Due upon receipt

QUANTITY	DESCRIPTION	UNIT PRICE	TOTAL
1	Business Services	55470	USD 47,470.00

SUBTOTAL	47,470.00
SALES TAX	
SHIPPING & HANDLING	
TOTAL DUE	USD 47,470.00

RECEIVED

Bank Wire Details:
Bank XXXX Federal Credit Union
Routing XXXXXXXXX
Account XXXXXXXXXX
Account Name: XXXXXXXXX

Anatomy of an effective Phish

On 2018-06-14 16:38, Arlene wrote:

Yes, we can do the special check run today and mail the check.

Just wondering if we have 3 bids for this service. How about the real estate services… Did we have 3 bids?

Thank you,

Arlene XXXX

Finance Director

XXX-XXX-XXXX

XXXX@XXXX.org

Anatomy of an effective Phish

From: Janet XXXX [mailto: mngt@XXXXmail.com

Sent: Thursday, June 14, 2018 7:34 AM

To: ArleneXXXX@XXXX.org

Subject: Payment

Importance: High

Arlene,

We don't have 3 bids for this service and the payment is requested by wire. The payment for this invoice is expected today. Can this you it now?

Janet

Anatomy of an effective Phish

On 2018-06-14 17:00, Arlene wrote:

We can do the wire transfer, same method as when we transfer the money to XXX.

Billy will prepare the paperwork, have you sign it and fax it to XXX Bank.

Thank you,

Arlene XXXX

Finance Director

XXX-XXX-XXXX

XXXX@XXXX.org

Anatomy of an effective Phish

From: Janet XXXX [mailto: mngt@XXXXmail.com

Sent: Thursday, June 14, 2018 9:45 AM

To: ArleneXXXX@XXXX.org

Subject: Payment

Importance: High

Arlene,

I am not currently available to sign for this, so please sign my name and process it.

Janet

Anatomy of an effective Phish

From: Janet XXXX [mailto: mngt@XXXXmail.com

Sent: Thursday, June 14, 2018 11:03 AM

To: ArleneXXXX@XXXX.org

Subject: Payment

Importance: High

Arlene,

Any update on the wire yet?

Janet

Anatomy of an effective Phish

On 2018-06-14 17:16, Arlene wrote:

Got it…

Thank you,

Arlene XXXX

Finance Director

XXX-XXX-XXXX

XXXX@XXXX.org

Anatomy of an effective Phish

Ultimately, the wire transfer for $47,470 was halted

- Policies were being bent
  - 3 bids
  - No executive signature
  - Urgency
- Other clues
  - Date stamps
  - Email addresses
  - Grammatical errors
- Luck and Intuition saved the day

The Security Audit:

- Interception of encrypted communications.
  - Insecure configuration of the email service allows attacks against encrypted protocols and could allow an attacker to intercept confidential data, such as user credentials.
- Eavesdrop communications between the clients and the server.
  - A remote attacker that has access to the network traffic between clients and the server can perform Man-in-The-Middle attacks against the website as it is not protected by a secure communications channel (HTTPS) in order to intercept confidential data, such as administrator user credentials.
- Attack outdated software.
  - A remote attacker may use publicly available vulnerability information and attack specific software (PHP, ExpressionEngine) that is outdated or no longer supported. Successful exploitation of publicly known vulnerabilities can result in unauthenticated remote code execution.
- **Solutions**:
  - Optimization of Patch Management
  - Periodic Internal and External Security Audits

Defense: No "Silver Bullet"

- Combination of defenses
  - Technological
    - ✓ Anti SPAM software
    - ✓ Blocking access to phishing URLs – Threat Intelligence
      - Site are often only active for a few hours
    - ✓ Web App Firewalls, Next Generation FW
    - ✓ Adversarial machine learning/artificial intelligence
    - ✓ Deception Technologies – CyberTrap, Attivo
    - ✓ Expensive to purchase, maintain and administer
      - The alternative is unacceptable risk

Defense: No "Silver Bullet"

- Combination of defenses
  - The "Human Firewall"
    - ✓ End users cannot be expected to recognize all manner of phishing attacks
    - ✓ Continual awareness training
    - ✓ Simulations – testing
    - ✓ Tracking improvements in the risk profile
    - ✓ Gamification – leaderboards and points
    - ✓ "Look for the Lock" is no longer very effective – Krebs on Security
    - ✓ Modern Risk Management Training platforms
      - Beauceron Security, Infosec Learning, ELC Information Security
    - ✓ Staff benefits in their personal lives as digital citizens as well

Kelly Robertson, CISSP

CEO, SEC Consult America

k.Robertson@sec-consult.com

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?

2018 User Risk Report

Speaker

Richard Bird, Chief Customer Information Officer, Ping Identity

Richard Bird is the chief customer information officer for Ping Identity. He has spent more than 20 years in corporate business, technology and roles within multiple industries. His diverse background includes serving as the CIO for one of the world's largest hedge fund administrators to being the CISO for a high-tech Swiss analytic device company. Richard's combination of IT operations and security have afforded him the opportunity to be recognized as an expert in identity-centric security, along with many other security domains such as threat and vulnerability management, as well as data and cloud security. An author and frequent speaker on a broad range of cybersecurity topics, Richard is widely recognized as an identity evangelist

Can we change user behaviors?

Richard Bird

Chief Customer Information Officer, Ping Identity

The Survey Says!!!

- The error rate of human behavior is
  - High (30% to 50%)
  - Painful (breaches, identity theft)
  - Consistently bad over time (it really isn't changing much)
- These facts have been confirmed continuously over the past several years
- Surveys by other security solutions providers confirm these findings

So what might this mean?

- Psychology, behavioral science, mathematics and anthropology clearly suggest that humans resist change – both actively and passively
- If Moore's Law has been advancing compute power exponentially for more than four decades but it takes years for humans to change basic patterns and habits, will awareness campaigns work?

  - Probably not – but security awareness training is still vitally important
  - The same 30% to 50% error rate in behaviors will remain consistent within our lifetimes and beyond
  - "Because it is the right thing" isn't a compelling argument or habit changer for humans
  - Customers and employees gravitate to the path of least resistance
    - ✓ Habits and rituals are those paths

How persistent and "sticky" are habits?

- Imagine an analog world where we required people to change;
  - Their house keys, car keys, storage shed keys, motorcycle keys and any other key they had in their junk drawer in their kitchen
  - For their house key, it must be a specific length and have no less than two square notches and two pointed protrusions
  - Their car keys must be both physical and remote (push button start) and both of them must be kept together at all times
  - Their storage shed keys can just be any old key – what's at risk in the shed?
  - Their motorcycle key must have an electronic chip
  - The owner can choose to have one master key that fixes this all, but also must change it every 90 days – good news though, all the other keys will be changed according to the rules every 90 days automatically

What are the two predictable behaviors for the vast majority of humans?

1. Nothing will ever be locked up, or
2. Everything will be tied to one master key – that once it has been copied or stolen results in a total compromise of house, car, shed, motorcycle and any other key (account) laying around

But in the digital world we expect entirely different behaviors

Surveys like this confirm that our expectations for change will always be at odds with the simple realities of human behavior

So what do we do?

- We need to recognize truths and facts that bind all human beings
  - Humans are strongly tied to their habits and rituals
  - This tie is so strong that patterns of behavior are virtually unspoofable (i.e. behavior as a biometric)
    - ✓ Habits and rituals do change with time, but slowly and in predictable ways
  - A radical break from habit and ritual is so uncommon that it becomes an easily recognizable anomaly
  - Behaviors that show no pattern associated with habit and ritual are almost always machine generated (i.e. bots)
    - ✓ The exception being certain human pathologies such as schizophrenia
  - Since habits and rituals are so tightly coupled to each person, the key to the future is identity-centric security

Sounds like you are trying to sell me something

- Experience gained from running one of the largest centralized identity security organizations in the world
- Virtually all identity solutions today rely on non-standardized, non-templatized, non-rationalized, unclean, corrupt data (i.e. Active Directory)
- We're collectively, corporately and globally "remembering" what we've always known in the analog – identity means everything when it comes to security

We can account for the nature of human behavior by focusing our technology on one simple question

Are you who you say you are?

- Identity-centric security frameworks are re-defining control structures
- Authentication (are you who you say you are) isn't a control, it is the control
  - The only inhibitor to this today is a reliance on the user and a dependency on known data (tokens, certificates, questions, verification codes)
  - And if it is known by us, it can be known/stolen by others
- In the very near future, 2FA and MFA will give way to "no FA" and "passwordless" identity control
  - Data driven continuous authentication (in-session)
  - Escalating and de-escalating privileges
  - Immediate session termination on aberrant (non-habit) behavior
  - Tightly couple correlative biometrics
  - The ability to isolate bad user behaviors – if you are who you say you are then monitoring out of band behaviors becomes an achievable reality

Instead of changing human behavior we focus on using human rituals and habits and augmenting with a nearly infinite number of useful data points (face/retina/finger, location, calendar schedules, travel arrangements, etc.)

ISSA

Information Systems Security Association International

www.issa.org

QUESTIONS?