Unprecedented: the disproportional rise in Internet activity

We're in uncharted territory. The world has never been so hyperconnected.

In the past four years, traditional banking methods, such as in-person branch visits or ATM transactions, have remained virtually unchanged. Meanwhile, online banking has steadily climbed each year and mobile banking has nearly doubled in four years to an adoption rate of 35%.1

The proliferation of electronic banking activity is the tip of the digital iceberg. Last year, there were 2.7 billion Internet users; this year, there are over 3 billion — that's roughly an 11% increase in users. But the increase in online activity is not proportional. Within the same year, Amazon sales per minute increased nearly 21%; tweets went up nearly 25%; approximately 76% more Instagram photos were uploaded; and the volume of content uploaded to YouTube each day increased 197%. There are more users every day, and each user is doing a lot more online. 2

That’s the upside of our hyperconnected reality. The downside is the increase in cybercrime. We’ve never faced such highly sophisticated adversaries. According to the Gemalto’s findings from the 2014 Breach Level Index report, 2014 saw a 78% increase in the number of breached data records, pushing the total slightly beyond 1 billion stolen records.3 This is unprecedented.

Unprecedented crime requires an unprecedented response

On February 13, 2015, at the first ever Cybersecurity and Consumer Protection Summit, President Obama noted, “the cyber world is sort of the wild, wild West — and to some degree, we’re asked to be the sheriff.” In this new role, the United States government has proposed unprecedented involvement in preventing, mitigating and punishing cybercrime. Among other measures, the government is seeking legislation to support more threat intelligence sharing between the public and private sectors. This new legislation encourages other critical sectors to share information in the same way banks have been doing for years. It also aims to bring the government into the loop so the private sector has access to government threat intelligence and vice versa.

U.S. Bancorp strongly supports this legislation. Once upon a time, our adversaries were mostly isolated hackers and organized crime gangs; today, financial institutions have to add nation states to the mix of attackers.

By ourselves, companies will have a difficult time mounting an effective defense against another nation’s military. Fortunately, we don’t have to go this alone. Cybersecurity is a team sport. Partnering with government agencies, Information Sharing and Analysis Centers (ISACs), and other organizations allows companies to protect the privacy of their data while remaining secure.

1 Source: Federal Reseve
2 Source: Techspartan
3 Gemalto 2014 Breach Level Index
The past several editions of The Shield have featured articles on email spoofing and masquerading schemes, dubbed Business Email Compromises (BECs) by the FBI. These types of fraudulent activities are an increasing menace to large and small businesses globally. To help you recognize the characteristics of these threats, two of the most common variants of BEC scams are outlined below. Each narrative is a fictitious account based on real-world events.

Scenario one: The CEO impersonation
The most common variant of the BEC scam. It requires the least amount of effort to be successful.

Pre event
In preparation to target “Computercorp” for their next scheme, the fraudsters:

- Perform reconnaissance, identifying the management structure as well as key individuals within the company who are the most likely to process financial transactions.
- Use Google and LinkedIn searches like “Computercorp controller” and “Computercorp CEO” to identify the key individuals, including the CEO “Judy Exec” and Controller “Henry Ledger”.
- Identify the email naming format for the company through additional searches, and discover Judy is on vacation through her social media account.
- Create a lookalike domain (cmputercorp.com) through an online marketing company that offers free trial domain registration and hosting. They then set up a lookalike email address (judy.exec@cmputercorp.com) to leverage during the impersonation.
- Generate a PDF with payment instructions to an account owned by them.

The scam
The fraudsters initiate the communication to the Computercorp controller, Henry Ledger, beginning the fraud scheme.

Initial email from fraudsters

```
From: Judy Exec <judy.exec@cmputercorp.com>
To: Henry Ledger <henry.ledger@computercorp.com>
Subject: Urgent payment

Henry,
What is the cutoff time for wires? I need to have this payment sent ASAP.
<Attached: PaymentInstruction.pdf>

-Judy
Sent from My iPhone
```

Response from controller

```
From: Henry Ledger <henry.ledger@computercorp.com>
To: Judy Exec <judy.exec@cmputercorp.com>
Subject: Re: Urgent Payment

Judy,
Wires must be processed prior to 2:00 PM PT. How should I code the transfer?

-Henry
```

Final response from fraudsters

```
From: Judy Exec <judy.exec@cmputercorp.com>
To: Henry Ledger <henry.ledger@computercorp.com>
Subject: Re: Urgent payment

Please code to my admin for now. Thanks.

-Judy
Sent from My iPhone
```

With this information, Henry initiates the wire transfer to the fraudsters’ account. Dual authorization is required. So, the secondary approver calls Henry, who confirms that the request came directly from the CEO and is urgent. The secondary approver also approves the wire.

- The money is sent to the fraudsters’ account.
BEC scam update (continued)

Post event
• Judy Exec, the CEO, returns from vacation and Henry sends her a note to reconfirm the allocation of the funds from the previous wire.
• Judy calls Henry immediately, claiming that she did not send any instructions for a wire.
• Henry contacts their bank to request a funds recall. The bank initiates the recall; however, the funds have already been moved from the fraudulent account and are no longer available.
• Computercorp contacts their local FBI field office and reports the fraudulent event to the Internet Crime Complaint Center (IC3).
In the aftermath of the event, Computercorp strengthens their wire authorization controls by implementing callback procedures for all requested wire transactions.

Scenario two: The payment instruction switch
Another scenario involves fraudulently changing a known supplier’s payment instructions to divert funds to an account owned by criminals or their accomplices.

Pre event
An organized crime group targets “ABC Corp.”, a U.S.-based global manufacturing company that makes frequent wire payments to foreign suppliers for goods and services. The group:
• Identifies one of ABC Corp.’s Asia-based suppliers, “XYZ Supply.”
• Compromises the email accounts of several XYZ Supply account reps who are using weak passwords in their web-based email solution, which has no secondary authentication.
• Search through the email for payment requests to customers of XYZ Supply and notice an invoice to ABC Corp. for goods, with an additional request for goods to be invoiced in the near future.

The scam
• The criminals email the supplier manager at ABC Corp., via the most recent XYZ Supply email chain requesting a change in payment instruction.
• The email does not alert the supplier manager given it is legitimately from the XYZ Supply email account.
• The supplier manager updates the payment system with the new account information assuming the email was legitimately sent from XYZ’s account representative.
• ABC Corp. receives the goods and pays via a wire to the fraudulent account provided by the criminals.

Post event
• The day after payment, the supplier manager at ABC Corp. emails the account representative at XYZ Supply to notify them of the payment. The account representative responds that the wire was not received.
• The controller checks the outgoing wires report to confirm the wire was sent, and ABC Corp. discovers the wire was sent to a fraudulent account.
• The controller at ABC Corp. calls their bank to request a funds recall, but the funds are no longer available in the receiving account and cannot be recalled.

ABC Corp. and XYZ Supply split the cost of the loss, and later implement additional controls around payment instruction changes including callback confirmation procedures. XYZ Supply also commits to implementing stronger security controls on their web-based email system, including multi-factor authentication.

Recap and defense
These scenarios depict situations that could have been avoided through stronger internal controls. In both cases, a phone call directly to the requestor via a verified number could have avoided the situation. While these situations vary in degrees of sophistication, stronger controls around email must also be part of every business’ security strategy. Keep in mind that traditional email should not be considered a trusted communication mechanism when dealing with critical activities such as money movement.

Additional best practices and information regarding this threat can be found in previous editions of this newsletter as well as the latest press release from the IC3.
Five tips for building a strong security awareness program

The best protection against cybercrime requires a two-part defense:

1. The right security technology in place to monitor systems, detect issues, and alert potential criminal intrusion; and
2. An educated work force. Every individual who interacts with key systems must understand and accept their role in cybersecurity.

Some of the largest data breaches seen in recent years began when a single employee opened a malicious attachment or link in an email and unknowingly infected their computer and the company’s network. The common denominator across the top four cybercrime patterns (accounting for nearly 90% of all incidents) is people, whether it’s goofing up, getting infected, behaving badly, or losing stuff.*

Any employee who opens email or uses the Internet is at risk of infecting your company. This facilitates the need for you to educate your workforce on the security behavior you expect from them, test them on what they’ve been taught, and create incentives to follow rules. Your company’s security will be the better for it.

Here are five tips to get you on your way:

1. Establish objectives
Define measurable objectives for the program and identify the measurable outcomes that map to them. This will foster real behavior change and gain executive support.

What do you hope to accomplish: A reduction in malware infections?; Greater adoption of secure document disposal?; A decrease in stolen company laptops?; Regulatory compliance?

Train employees to report phishing attempts and other suspicious behaviors. Include training on reporting these types of activities to your security event center. Then track the metrics.

2. Make it mandatory
In many large corporations, security awareness training is mandatory. No one is exempt. If you want results — make it mandatory

Example: Employees who fail to complete the required training are singled out for “escalation.” Their managers are notified, then their manager’s manager, and on up the corporate ladder until the situation is resolved.

3. Enforce security policy
Set up a security policy that contains strict rules for protecting confidential data — on paper, online, and in conversations — and enforce it! Your policies should map to a disciplinary baseline. Leverage mandatory security awareness training to ensure everyone understands the policies and the consequences to violators.

Example: You have a policy stating company data downloaded to electronic media must be encrypted; clearly state what the consequence is for violating this policy.
4. Create a security culture
Weave security messaging into your company's physical and online space.

- Feature security articles and tips on your company’s website and link them to credible consumer sources, such as FBI Scams and Safety page, Internet Crime Complaint Center (IC3), Stop.Think. Connect.
- Display topic-related posters around the workplace.
- Hire outside speakers who specialize in security awareness.
- Hold education sessions on security topics.
- Host games and contests for recognizing phishing emails.

5. Encourage a security mindset
A security mindset means security is second nature — no matter where you are, what you’re doing or what device you use. For example, it means:

- you create strong passwords whether it’s required by the application or not;
- you lock screens without thinking twice;
- you always treat links in marketing emails cautiously.

A security mindset is great for business. But, employees that follow good security practices in their personal lives carry these habits into the workplace, and vice versa. Go beyond office-based rules to offer employees advice on how to protect themselves at home. You can provide tips on:

- protecting your children on social media sites,
- protecting parents and grandparents from elder fraud, and
- setting up alerts for their online banking devices.

A security awareness program that blends in tips and best practices for an employee’s personal life will be more effective than an exclusive focus on business.

By following these tips, you’ll be on your way to defining your own security awareness program and better protecting your business. And remember — Security awareness is not actually about being aware — it’s about changing behavior.

* 2015 Verizon Data Breach Incident Report