



A Phish Tale: What a Successful Attack Looks Like *by Dan Callahan*

It's instructive to see how a successful phishing attack can happen. Let me share a story with you. I got a text message, then a call last week. Both were from the same customer. "Dan, I think my account has been hacked," was the message. "What do I do now?" The customer went on to say that he figured out his account had been hacked when he began getting calls from people, asking him why he'd sent them a message about an overdue invoice.

I was in the car, so I told the customer to unplug from the Internet and scan his computer right away. Once I got to a computer, I changed his account password. As I continued to work with the customer, I began to see how this successful phishing attack happened.

First Comes the Phish

Jim (not his real name) told me that he had recently received a message and clicked on the link in the message. He wasn't sure what happened next but thought that maybe he'd

given up his username and password by accident.

As we checked the security logs, we determined that someone accessed the account around the time Jim clicked on that link, September 17th. There were first some unsuccessful attempts to access Jim's account from IP addresses in Asia. Seven hours later, there were successful login attempts from Europe. Five hours later, there were other successful logins from Africa. It's possible the IP address locations were spoofed. It's also possible that Jim's account credentials were now on some dark web database and being exploited.

Next Come the Outlook Rules

The next step in this successful phishing attack occurred when the Bad Guy created some Outlook rules designed to hide their activity. Clearly, they were planning to use Jim's account for some time. The Bad Guy created rules to

- Delete sent messages
- Delete any undeliverable messages
- Send any replies to an obscure folder
- Forward all messages to (presumably) that Bad Guy's Gmail account

Jim's account had been hacked for a week before he noticed. And he only noticed when people started asking him why he was sending them a note about a past due invoice (Jim doesn't work in Accounts Receivable). These Inbox rules hid any signs that something was wrong.

Continued on Page 6

How Secure Is Your Attack Surface?

by Tim Haight

Recently, CGNET has begun to offer attack surface assessments in addition to internal and external penetration testing. I thought I'd tell you why.

Conventional penetration tests, such as Nessus or QualysGuard, do a terrific job of detecting vulnerabilities on servers. Regular use of these tools has become a best practice, with good reason.

Unfortunately, in the same way that rust never sleeps, malicious actors are constantly looking for new ways to get into your systems. Now that hacking has become big business, malicious researchers have plenty of resources to devote to discovering new methods.

Continued on Page 7

Take a Look Inside:

Social Engineering	2
Mobile Phishing	3
Security Training Engagement..	3
Transitioning Skype to Teams ..	4
Password Managers.....	5
Tips for IT Assessments.....	10
Who is CGNET	12
Comparing Cloud Services	13
Cybersecurity Tips	14
A Message from the CEO	16
Meet the Bloggers	16

The Treacherous World of Social Engineering: Top Tricks of the Trade

by Jackie Bilodeau

Hacking is a thriving business. We hear about it in the news all the time these days. When we think of a hacker, we imagine a computer whiz who has the technical expertise to “break in” to computer systems. The high school nerd who works his way into the school’s admin computer to change grades. The tech genius who has the know-how to hack into government systems to wreak havoc or steal data.

But there is another type of hacker who uses an entirely different set of skills to get the information they want. They are the social engineers: hackers who exploit aspects of human psychology to ensnare their victims and trick them into getting what they want.

Social engineering utilizes a broad spectrum of methods – none of which are mutually exclusive. I’m going to help you get familiar with some of the most common tactics. That way you can be on the lookout for yourself and also help educate



other members of your organization.

Phishing

You’ve likely heard the term “phishing” by now; this is the most common type of social engineering attack. The bad actor uses email, social media, instant messaging, texting or phone calls to trick their victims. The goal: Getting them to give up private information or visit a malicious website that will compromise their system.

These social engineers are very good at replicating messages from official-looking sources. They can spoof logos, images and texts to look nearly identical to a legitimate source. However, there are some telling signs you can look for.

Phishing tip-off #1: Urgency

Any message expressing urgency of action – particularly an action that requires providing private or financial information -- should be questioned. The hacker is *playing to your fears*: X has happened and you should do Y immediately to correct the problem (see Example below left.)

Phishing tip-off #2: Mismatched addresses

Check the **sender’s address** as well as **link addresses** within the message. If not from a legitimate source, you may discover the “from” address is not what it initially appeared to be. (For example, a number “1” is substituted for a lower-case letter “l”.) Or there is some other hard-to-catch-at-a-glance minor spelling error, like an extra letter. In less sophisticated cases, hackers don’t even bother to mimic a legitimate address; they just assume you won’t notice.

Also inspect any links within the body of the message they are trying to get you to click on, to reply to. If it is completely different from the sender’s in the “From:” line, be wary. Even trickier: the URL you are to click on *looks* the same as the sender’s “From:” address. But in fact, it is *hyperlinked* to a different destination altogether. (If you hover your cursor over the link the true URL will appear.) Bottom line: Do NOT reply or click on anything until you’ve thoroughly inspected any and all addresses in the message!

But while phishing in its various forms is the most common form of social engineering, there are others to look out for.

Pretexting

Pretexting is a form of social engineering where the hacker

Example

From: Amazon managment@mazoncanada.ca Wed 10/30/2019 10:29 AM

<Note the misspelling of Amazon in the address>

To: Jackie Bilodeau

Subject: Suspension

amazon.com

Dear Client, ← **Generic, non-personalized greeting**

We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else in order to prevent any fraudulent activity from occurring we are required to open and investigation into this matter. We’ve locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html> ← **Hovering over the link reveals it actually points to:**
<http://redirect.kereskedj.com>

Sincerely,

The Amazon Associates Team

© 1996-2019, Amazon.com, Inc.

Continued on Page 4



Challenge: How to Foster Security Training Engagement *by Dan Callahan*

If you've been following along (and we know you have!), you've heard us stress the importance of security training for staff as a component of your cybersecurity posture. But conducting a training session is not enough; it has to stick. So, how can you foster security training engagement? How can you get your staff leaning forward and really participating?

We've all been through bad training. I recall the time at another company when our HR representative literally stood with her back to the audience, reading the text of a PowerPoint slide. That sort of cringe-worthy experience is not what you want to replicate with your cybersecurity training. Luckily, research by Britt Andreatta and others has shown that breaking the training into short pieces, and engaging the brain in different ways, will help participants learn and retain more information.

Solution: Pop Quiz!

There are lots of ways to foster security training engagement.

We've done this in the past with exercises like "build a phishing email" and our security version of Family Feud ("survey SAYS!"). These exercises all help to foster security training engagement. The method we're going to talk about here is simple. Recently a customer showed us a new approach: online quizzes.

Let me start with the "aha!" moment. My co-presenter for the security training pointed out that using an online quiz (vs. calling on people to answer) had two benefits.

- More people participated, because they were responding anonymously. Some people are just shy.

Phishing in Your Users' Pockets

by Tim Haight

You may be confident that you've conquered phishing in your users' office email, but how are they doing on their phones?

In the latest Verizon Data Breach Investigations Report, click rates on malicious emails declined from more than 20 percent in 2012 to less than three percent in 2018. Awareness of email phishing seems to be taking hold.

At the same time, however, the figures showed that 18 percent of clicks on phishy links or attachments are now made on mobile devices. Mobile security specialist Lookout said in 2018 that the rate at which people are falling for phishing attacks on mobile has increased an average of 85 percent every year since 2011. It's clear that mobile phishing is a major problem now and probably will only get worse.

Why Mobile Phishing Works

Mobile hardware makes it easier to fool users. So does the software, and, most importantly, so does the way people use their mobile devices.

As Arun Vishwanath, Chief Technologies for Avant Research Group puts it, "Mobile devices have relatively limited screen sizes that restrict what can be accessed and viewed clearly. Most smartphones also limit the ability to view multiple pages side-by-side, and navigating pages and apps necessitates toggling between them – all of which make it tedious for users to check the veracity of emails and requests while on mobile."

Mobile operating systems and apps also limit what the user sees and make it harder to protect against phishing. Many apps limit how much of the email header is visible. The email source information may not be accessible at all. Meanwhile, as Viswanath says, mobile graphical user interfaces "that foster action – accept, reply, send, like, and such" make it easier for users to respond quickly to a request. "On the one hand, the hardware and software on mobile devices restrict the quality of information that is available, while on the other they make it easier for users to make snap decisions."

The variety of apps susceptible to phishing, or smishing (SMS phishing), or vishing (voice phishing) are greater on smartphones, too. There are lots of different interfaces

Continued on Page 10

Continued on Page 11

Going from Skype for Business Online to Teams

By Dan Callahan

Microsoft has announced that Skype for Business Online will be retired as of July 31, 2021. This retirement is not a surprise. I've written before that it was clear Teams would be Microsoft's collaboration platform and that Skype for Business Online would be retired at some point. Well, that point now has a date. If you're using Skype for Business Online, it's time to plan your Skype for Business Online to Teams transition.

Before I continue, I'll note that Skype for Business Server and the "consumer" version of Skype are not affected by Microsoft's announcement. If your organization uses Skype for Business Online, you're wondering how much work it will be to switch to Teams. That question turns on whether your organization is using telephony or not. And by "telephony" I'm referring to the ability to make a voice call to a regular telephone number. Think, calling the caterer down the street to arrange for lunch to be brought in.

Skype for Business Online Transition without Telephony

This is the simpler case to consider. If you're using Skype for Business Online with just its included features—chat, IP voice, IP video—then there's little to do. You'll add new users directly to Teams. Everyone (old and new) can use Teams via its web app or via the downloaded app. You'll determine what "coexistence mode" in which you want to run Teams and Skype for Business Online.

Continued on Page 12

Social Engineering

Continued from Page 2

maintains a fake persona to trick their victim. Unlike phishing, which plays off fear and urgency, pretexting works from a false sense of trust to extract information. In essence, setting the "pretext" of a trustworthy relationship between scammer and victim.

A scenario using the pretext technique might go something like this:

The scammer has already – via phishing or by some other means – gathered enough personal information on a member of an organization to create the pretext of being a person of some authority within that company. He or she then calls the IT Help Desk pretending to be that person with a made-up problem. Already armed with personal information and therefore appearing trustworthy, he requests further personal information needed to resolve the phony problem.

The difficulty in protecting your employees from this type of scam depends on the size of your organization. If you are a smaller company, it's pretty easy to know if someone who says they work for your company actually does. But this is much more difficult if you have a large organization. In that case, unfortunately, the best bet is to trust no one! Have staff request employee ID numbers when requests are made, and then separately vet the person before providing any further help.

But no matter the size of your organization, if a person claims to be from *outside* the organization but with permission and/or authority to gather data, instruct your employees to be proactive in checking out their identity. (Again, trust no one.) Get the person's name, company name, phone number, etc., and use every tool at your disposal to verify, verify, verify!

Baiting

Baiting is in many ways similar to phishing. However, this form of social engineering is counting on a person's natural curiosity and desire to get something for free. Baiters may offer users free music or movie downloads, if they give them their login credentials to a certain site. (Of course, the only free thing they will get is a world of headaches!)

Some baits rely only on the element of human curiosity. The perfect example of how little it takes to trigger this natural reaction and potentially bring great harm to an organization was demonstrated back in 2006:

A network security firm hired by a credit union to assess their network came up with a simple, clever way to bait employees into unwittingly giving them private data from their computers. They scattered 20 USB drives – set up with a Trojan virus to collect passwords and other information -- throughout various areas of the facility frequented by employees (parking lot, smoking areas, etc.). They then stood back and watched as *every single* USB drive that was picked up (15 in all were found) was brought inside and popped into employee's desktop machines! As the employees scrolled through the images planted on the drives, they did not know they were simultaneously sending all sorts of private data to (fortunately, in this case) the security team.

Quid Pro Quo

Although a lot like baiting, quid pro quo attacks are more transactional (as the name implies: I'll do something for you if you do something for me.) Generally, the hacker is offering a service in exchange for an action that will supposedly make it possible. A common example is the hacker impersonating an IT staffer within a large organization, (see pretexting above), they call up an

Continued on Page 6

Password Managers: For Convenience *and* Peace of Mind

by Jackie Bilodeau

Recently I began assisting our Global Services VP, Dan Callahan, with Security Training at customer sites. (Yes, my job title is Communications Director. But at a small company like ours, we all wear many hats.) While I work for an IT consulting company, I'm still on a learning curve when it comes to some aspects of IT. So, I admit to having had a few "aha" moments during these sessions. I personally thought I was pretty savvy when it came to the safety and security of my online data. But it turns out I still had a few things to learn, particularly when it came to keeping my passwords safe.

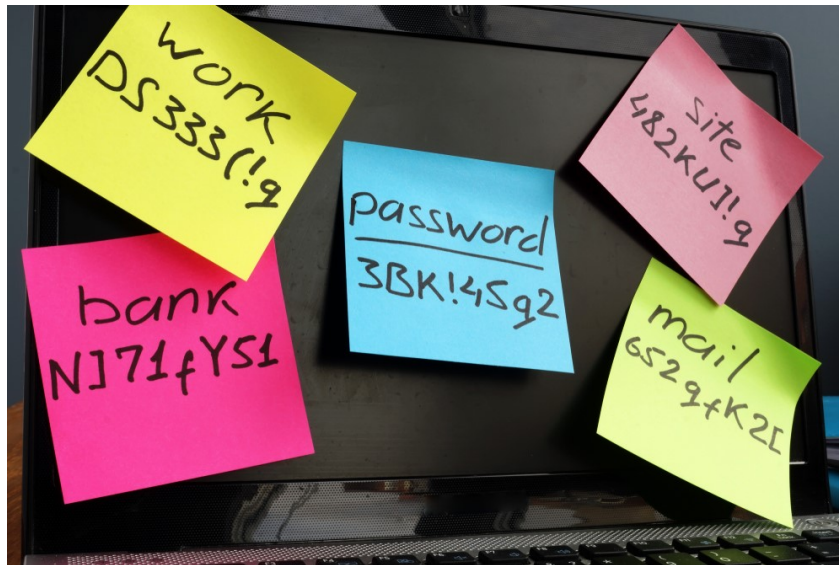
For example, saving all my passwords in my browser (Google Chrome, in my case) is a rather risky proposition. (Or as Dan put it rather emphatically when someone asked about this during the training, "Oh no, you should NEVER save your passwords in your browser!") Why? Because (in my case) all it would take is for someone to hack my Google account and they would have access to every password for every site I've ever saved on my laptop, phone and tablet. Yikes. And lest you non-Chrome users think you're safe, the same is true for other browsers. It's kind of scary when you think about it.

The problem is, I like the convenience of having all my passwords saved in one place. Call me lazy, but I especially like it when my browser fills them in for me when logging onto a website. This is where password

managers come to the rescue.

Lock 'em up

Like a browser, a password manager saves all your passwords in one place. You only need to remember one master password or phrase (make it complicated yet easy enough for you to remember, like song lyrics or a line you've memorized from a book. Throw in a couple of numbers replacing letters to make it even more complex). But how is it any different from just using your browser, you



ask? Well, password managers are like a bank vault for all your passwords. Their primary purpose is to secure your passwords like they're the gold in Fort Knox. And if someone DOES hack the password manager site (yes, it has happened), the damage is mitigated by the simple fact that all the passwords they've saved for you are encrypted, making them virtually meaningless to the hackers who've gotten hold of them.

On top of storing all your various passwords in a super-secure location, password managers have other benefits: They can generate very complex and unique passwords for you that you will never have to memorize. Additionally, many password

managers sync your password database across all your devices. That way you have immediate access to your passwords on your desktop, laptop and mobile devices when you are ready to log in. And most come with extensions that autofill your passwords for you on login pages. Lazy folks like me can rejoice!

Time to be proactive

I decided the time to find and start using a password manager was now. I read several reviews on the

various password managers available, and after settling on 1Password, I subscribed via the iPhone App store. Their current pricing is \$3.99 a month, but if you pay upfront for an annual subscription at \$35.99, (hold on, I'll do the math for you), it comes out to only \$2.99 a month. Seems like a pretty fair price for peace of mind, no? 1Password apparently was started as a

Mac-centric password solution, but it has since expanded to include iOS, Android, Windows, and ChromeOS. This is good for me, as at home (and on-the-go) I'm a Macbook/iPhone/iPad person, but at the office we're all about PCs and Windows.

I know others here at CGNET who use Lastpass and RoboForm, and someone once recommended Dashlane to me. But you can read up on the features and reviews and decide which one is best for you.

Bottom line: Get on top of this! Like me, once you have, you will sleep easier at night knowing that access to your personal data is far safer today than it was the day before. 🍏

A Phish Tale

Continued from Page 1

In fact, when we looked at Jim's RSS Feeds folder, we found a thread between him and the Office Manager, asking that a \$20,000 invoice be paid right away. The initial request and all the replies were tucked away in a folder Jim would never look at. Fortunately, the Office Manager didn't fall for the scam.

The Final Step: Deliver the Payload (Rinse and Repeat)

When I ran a message trace on Jim's account, I found that the account had sent out 430 messages over the prior 48 hours. The Bad Guy spammed Jim's entire contacts list a phishing message with the subject "60day Past Due Invoice." (If you've been to any of my security training sessions, you'll recognize the subject line as trying to create a sense of urgency for the victim, to get them

to open the message.) We don't know whether the messages were attempts to get money, spread more malware, or both.


Lessons to be Learned from a Successful Phishing Attack

Jim works for a small company. They have no IT staff and run on a lean budget. How can a company like this protect itself from a successful phishing attack?

- One of the best protections is to adopt Multi-Factor Authentication (MFA). This remains the best way to stop most phishing attacks. MFA requires "something you have" as well as "something you know." It may be easy to acquire your password (something you know). It's much harder to acquire or tap into your mobile phone (something you have).
- Set an alert that notifies an administrator whenever an

Outlook rule is created that forwards mail outside the organization. Seeing and reacting to such an alert would have stopped this successful phishing attack much sooner.

- Get smart about phishing attacks. Train users to recognize the signs that an email may be suspect.
- Protect users from themselves. Services like Office 365's Advanced Threat Protection can "sandbox" URL's found in an email, preventing the user from following a bad link.

Organizations of all sizes are potential victims of a successful phishing attack. In fact smaller organizations are lately being targeted for these attacks, because they lack the resources to prevent them or fend them off. These simple steps can help any organization better defend itself against phishing attacks. Don't wait to start adopting them! 


Social Engineering

Continued from Page 4

employee (well, perhaps several employees until one takes the bait) claiming that they need their help in order to administer a software upgrade for their team that some "higher up" requested for their team. They ask the employee to do something to make that possible (supply some password or turn off a firewall). The employee believes they are doing something to help the IT staffer fulfill his obligations AND are get something in return. In reality, they are allowing the bad guy in to do something altogether different (install not an upgrade, but malware).

Don't become a social engineering victim!

Pay attention to these tips:

1. Consider the source – and then check it out. If little red flags went up while you were reading a message (based on some of what you read above, or just your genuine human intuition), click on *nothing*. Leave email (or the text, if on your phone), and use your browser to check out URLs, or just go directly to the main website of the organization supposedly seeking your input and proceed from there.
2. Slow down. Re-read. Look for errors in spelling, wording or anything else that seems "off".
3. If it sounds too good to be true – or in some cases, too *strange* to be true – it probably is. Investigate and verify. (See: Nigerian prince email scam, which has been around for a long time. And continues to rake in big bucks to this day!)
4. And it should go without saying: Make sure you have anti-virus software or a security suite installed and that it is up to date on all of your devices! 



How Secure Is Your Attack Surface?

Continued from Page 1

What Is an Attack Surface?

An attack surface assessment addresses many of these new approaches. The classic definition of an attack surface is the sum of the different points where an unauthorized user can try to enter data or to extract data from a software environment. Penetration testing covers some of these points, but an attack surface assessment's scope is broader.

For example, a recent assessment we did with our partners Hacker Target revealed several interesting items we would not otherwise have encountered. One was an old website that the client had previously used. While no domain name pointed to it, it was still on the internet. It was using a now very old version of a content management system, which meant it was full of unpatched vulnerabilities.

It's possible to argue that an old site isn't

important but think what could be there. There could be old username/password combinations that were reused in the new site. There could be old data that had not been removed but which was still revealing. Possibly, there might be email addresses listed in plain text. A diligent hacker could find out many things to apply to the new website and the broader organization.

We might have caught this using nmap, but it's easy to simply assume that the client knows the IP addresses of all the endpoints exposed to the internet. Better to check.

Who Has Your Email Address?

Speaking of email addresses, this is another area where some additional research, such as that in an attack surface assessment, can help. A great number of email addresses have been captured by malicious hackers in previous adventures. These are often listed in databases and other places on the dark web. Sites like haveibeenpwned.com and others

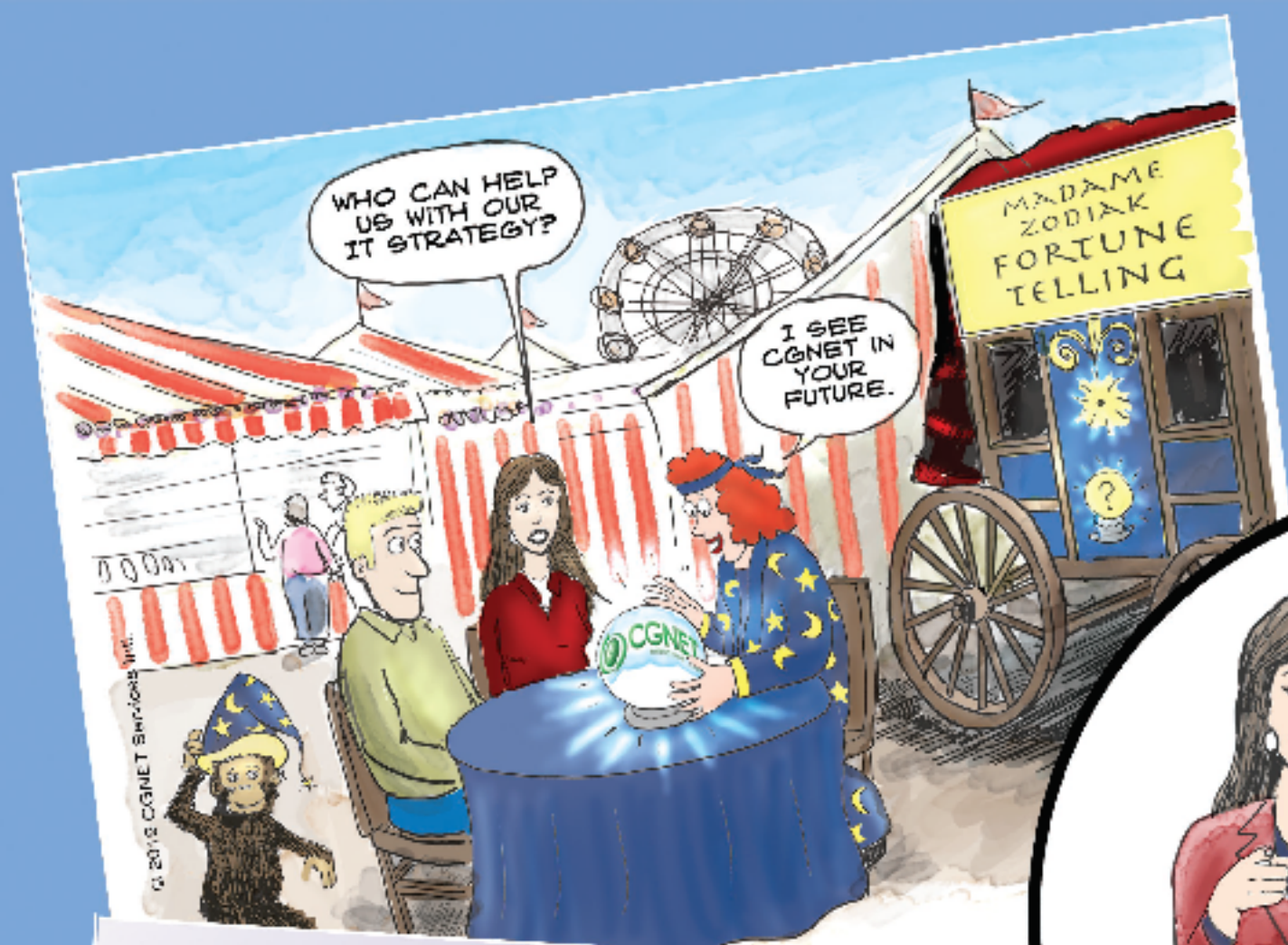
keep track of some of the emails that have been harvested. Other sites do as well.

Once somebody has your email address, they can send you spam, or they can send you phishing messages. They can use email enumeration to identify sites where your email addresses is a valid username, then they can use brute-force password attacks to find out your password.

A good attack surface assessment will identify which of your email addresses are available to malicious hackers.

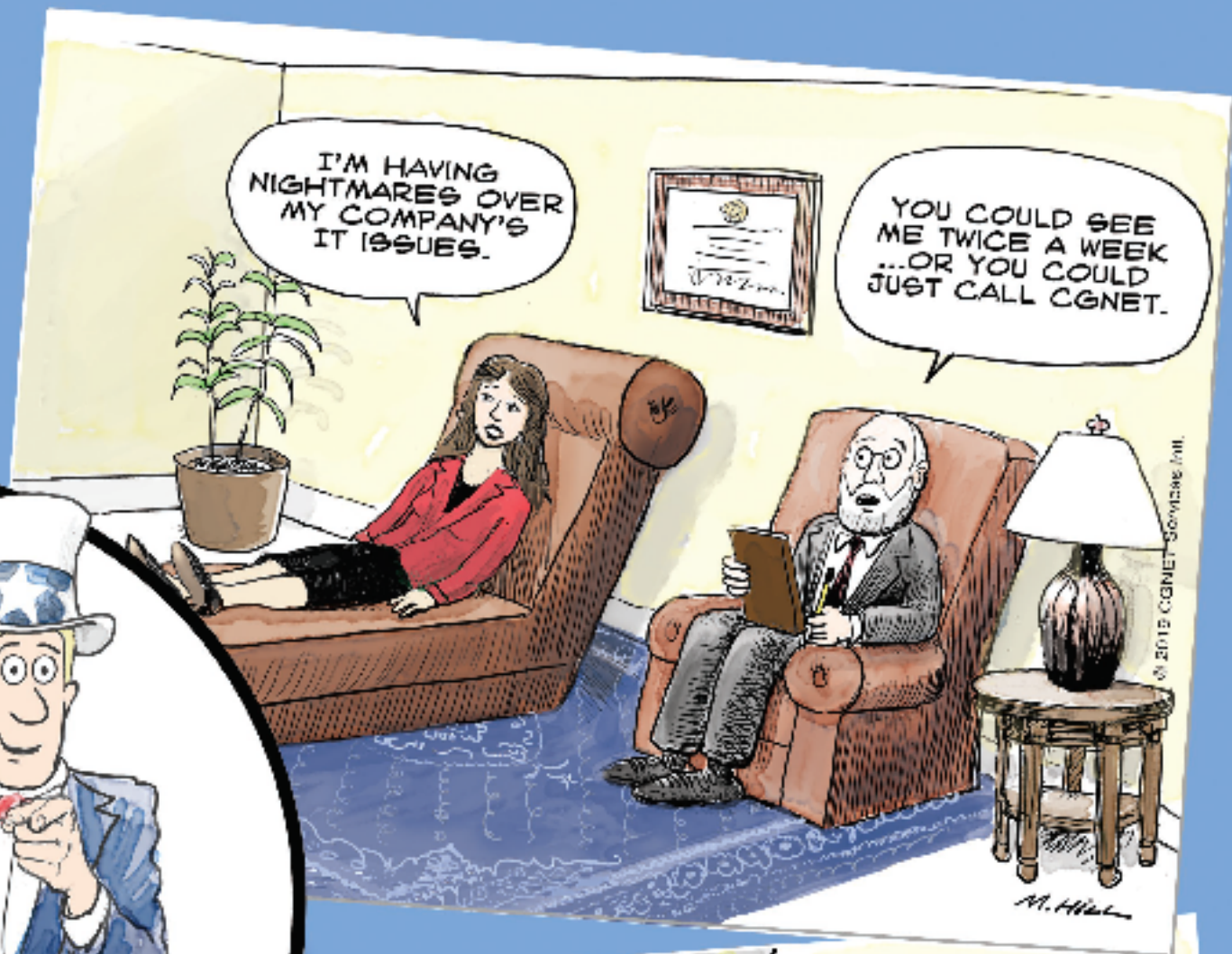
Bypassing Your Firewall

Another thing the assessment found was that the website's application firewall could be bypassed by working from discovered endpoints. I could go on, but this is becoming too long. Suffice to say that there are several more interesting things attack surface assessments turn up that a traditional penetration test may not find. Do some internet research about it. You may have found a new security tool. 🕒



**WANT YOU
SUBSCRIBE TO
CGNET BLOG!**

Click the link and click [Subscribe!](#)



Phishing in Users' Pockets

Continued from Page 3

within which you must look for phishing clues.

Don't Drive While You Text

By now, most of us are aware of the dangers of texting or checking your email while driving. But what about the effect of driving on how carefully you examine your text or email for phish?

For that matter, what about all the other things your users do while their smartphones are close at hand? Fill in your favorite here....

If you've noticed how quickly some people can switch between phone apps, such as different chats, you can see how they can't have much time to pay careful attention to whether a message is real or fake. Many people also wake up to the sound of an email, text or call. How alert are they then?

As Viswanath summarizes, "The confluence of design and how users interact with mobile devices make it easier for users to make snap, often uninformed decisions - which significantly increases their susceptibility to social attacks on mobile devices."

What's a User to Do?

Many of the recommended ways to fight mobile phishing aren't that different from what you do with PC email phishing. They're just a bit harder. For example, you can't hover your mouse over a link and see the URL. There is no mouse! In iOS, at least, you can touch and hold a link and get a similar display. For Android, the subject appears to be stimulating a debate among enthusiasts, with the typical clunky solutions.

The kind of advice that Apple gives for how to fight phishing is truly little

different from general warnings. On a support page, Apple suggests these things to look out for in phishing emails or texts:

- The sender's email address or phone number doesn't match the name of the company that it claims to be from.
- Your email address or phone number is different from the one that you gave that company.
- The message starts with a generic greeting, like "Dear customer." Most legitimate companies will include your name in their messages to you.
- A link appears to be legitimate but takes you to a website whose URL doesn't match the address of the company's website.
- The message looks significantly different from other messages that you've received from the company.
- The message requests personal information, like a credit card number or account password.
- The message is unsolicited and contains an attachment.

What Is the Advice Worth?

Several of these things, however, may be harder to do on a phone. For example, what about one of those alerts that pop up on your home screen and happens to contain a short link? Not only are abbreviated links a great way to hide unusual URLs, but also you don't even have the context around the alert.

At this point, the most sensible answer to me is not to click on anything in emails or chats you're not completely certain about while you're on your phone. Wait until you get to your PC. If you're still using one, that is. It looks as if the industry still has a lot to do to counter the mobile phishing threat. 🌀

Tips for IT Strategic Assessments

by Tim Haight

Anybody can do an IT strategic assessment and make recommendations. The trick is to get your recommendations accepted. This means really knowing what the organization wants and what it's willing to accept. To achieve this, your communication has to be great, both in what you put out, but, more important, in what you take in.

I come at this as an outside consultant, but I think some of what I say applies to internal studies as well.

The basic idea of an IT strategic assessment is straightforward: Examine all aspects of an organization's IT operation, compare that to best practices, and make recommendations, usually inside a roadmap for three to five years.

Organizations, however, can have lots of reasons for doing an IT strategic assessment. Some have a new president with different attitudes towards technology. They may want to focus on one part of their IT effort, such as implementing an important application or upgrading their infrastructure. Sometimes, they're moving to a new office. Some have had some major IT failures or security issues they want to avoid in the future.

The Beginning is Crucial

So, lots of reasons, and it's great to really understand them at the beginning. Sometimes, you will. The universal goal of an IT Strategic Plan is to align IT's activities with the specific goals of the organization, in the timeframe under discussion.

Continued on Page 15

Security Training

Continued from page 3

- Remote meeting participants could join in as easily as those in the meeting room.

How We Incorporated Quizzes into Our Training

Let's set the stage.

One of our customers noticed that click-through rates on its periodic phishing test were going up. (Did I mention that conducting regular phishing tests is also an important component of your cybersecurity posture?) Maybe this was because the customer had recently added a lot of staff. Maybe people were reverting to old habits. The customer asked CGNET to come in and conduct a security training session.

My co-presenter on the customer side thought we should focus on one or two topics and go in depth. In the past, we had tried to squeeze a lot of topics into the allotted time. Almost without fail, the result was that we couldn't spend enough time trying to foster security training engagement.

After some discussion, we agreed to focus on phishing. We wanted to spend the bulk of our time looking at example phishing messages and helping people understand the clues to recognize that they were fake. We used as many examples as we could of phishing messages actually received by the customer. We thought these "real world" examples would help foster security training engagement.

Following is an example message (not one received by the customer). Our plan was to show each phishing email and ask the audience any of three questions.

1. What are the clues that this message is a phishing message?
2. Guess what information or assets is the phishing person attempting to obtain?

3. What emotion is being targeted in this message?

We wanted to use an online quiz tool to ask these questions and share the response statistics. We thought about using something like Forms, since it can be used within PowerPoint. But we chose a tool called Mentimeter for the following reasons:

- My co-presenter had a paid Mentimeter account, so we could access more goodies like multi-part questions.
- Mentimeter works with a web browser and is optimized for mobile. We didn't want to spend precious training time working with the audience to download and install an app.
- We wanted our remote participants to easily join in the fun.

Quizzes Helped to Foster Security Training Engagement

Using Mentimeter to foster security training engagement worked well for us. We often had 80% or more of the audience participating. When we went over the quiz results, we generated additional comments and conversation.

From: Microsoft office365 Team [<mailto:cyh11241@lausd.net>]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account



Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify.

[Verify Now](#)

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

EXAMPLE

Mentimeter is designed to be a presentation vehicle with quizzing options. (It made me think of Prezi). Had we used Mentimeter that way, we wouldn't have had to shift between Mentimeter in a browser and PowerPoint. However, it was going to be too much work to recreate all the PowerPoint material in Mentimeter. So, we lived with the application-switching.

Here's an example of how the quizzes worked. These screenshots are from Microsoft Forms, but the user experience is similar to Mentimeter.

This is the question I wished I had asked in a quiz:

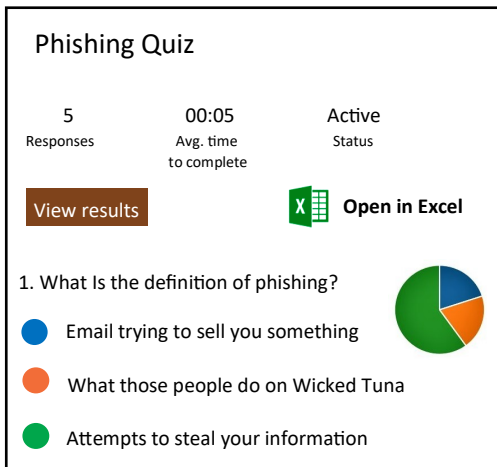
Phishing Quiz

(Sample quiz to go with phishing class)

1. What is the definition of phishing?
 - ☐ Email trying to sell you something
 - ☐ What those people do on Wicked Tuna
 - ☐ Attempts to steal your information

Continued on Page 12

And here is an example result:



Had I used a quiz to foster security training engagement, I would have more easily learned that no one — *no one* — understood my reference to Wicked Tuna (a tv show on the National Geographic network).

Be sure to look at online quizzes to foster security training engagement. They're fun and help you reinforce key training messages. They encourage friendly competition and audience dialog. They'll help your users be better email and web consumers. They'll reduce your cybersecurity risk. 🎯

CGNET was founded in 1983, as the result of an international effort to provide computer-based communication to an international development organization, the CGIAR. The concept spread rapidly to UN agencies, nonprofits, foundations, and NGOs. The early days are documented in the book: *The CGNET Story : A Case Study in International Computer Networking* by Selcuk Ozgediz, K. Novak and G. Lindsey (1994, Paperback). In the last decade our customer base has expanded to start-ups in the Silicon Valley, in particular the medical devices space.

- “Skype for Business Only” mode. Or as I like to call it, “Head in the Sand mode.” Skype for Business alone is used to deliver collaboration services.
- “Teams Only” mode. Teams alone is used to deliver collaboration services. This is where you're headed.
- “Islands” mode. This is the default coexistence mode. Skype for Business Online and Teams will exist side by side. Users will use each client app for their respective services.
- “Skype for Business with Teams Collaboration” mode. This coexistence mode is primarily intended for customers with Skype for Business Server installations. It allows for some interoperability between Skype for Business and Teams.
- “Skype for Business with Teams Collaboration and Meetings” mode. This mode shifts the meetings features from Skype for Business to Teams.

We recommend starting with the “Islands” mode when planning your Skype for Business Online transition.

Who is CGNET?

We provide organizations with best-in-class information and technology services. We are both a consulting company and a managed services provider. We are a California-based C corporation and have been profitable for 36 of our 37-year history. We provide services in four main areas:

- Cyber Security
- IT Management and Services
- Technology Strategic Planning
- Cloud Services

We have a staff of 30 located in California, Texas, North Carolina, Nigeria, Ethiopia, India, South Africa, and Chi-

na. Use this mode and get people going on Teams as quickly as you can. Yes, using Skype for Business Online for chat and calling while using Teams for channels and conversations is clunky. But we feel that users will want to move to Teams more quickly as a result. Once you've reached a “critical mass” of users on Teams, you can switch to Teams Only mode and move the remaining users over to Teams as well.

Skype for Business Online Transition with Telephony

I wrote an extensive piece about planning for Teams Telephony. You can find it at <https://cgnet.com/blog/get-teams-calling-details-right/>

If you're already using Skype for Business Online and Telephony, your planning has already been done. You'll have to choose which coexistence mode to go with as described above. In addition, you'll have a few other things to think about:

- Phones. If you have phones that you use with Skype for Business Online, you'll have to confirm that they will work with Teams. Chances are good that the same phones will work, but chances are

na. Our customer base comprises about 200 organizations in 130 countries. Our staff are diverse and highly trained.

We routinely do vulnerability and penetration testing and we conduct four to six major IT Assessments and/or Security Assessments per year. We have moved upwards of 14,000 users from on prem facilities to Azure, AWS. We support email for about 30,000 users and are business partners with Microsoft, Cisco, Hewlett-Packard, Symantec, Amazon Web Services, VMware, and Computer Associates. 🎯



Comparing Cloud Services...or Not

By Tim Haight

Now that everybody is moving to the cloud, quick or slow, I thought I'd spend a little time complaining about the state of good information to support your cloud services choices.

Microsoft Azure and Amazon Web Services (AWS) both have basic guides for pricing servers and related services. These can be useful. Of course, before being able to get useful information from them you must know your needs clearly. You also must be aware of various discounted pricing plans.

It seems that if you activate all the possible Azure or AWS discounts, the price difference between the two for basic access to servers is about the same.

The Plot Thickens

But what about more complex situations? My colleague, CGNET CTO Ricardo Uribe, pointed out the virtue of Azure if your organization is planning to host applications in the cloud. If you also have Office 365, the Azure AD directory services you would need for the applications is already included with Office 365. Such helpful tidbits are not always easily available from the vendors.

And what, perchance, if your situation involves other vendors, such as Oracle? We recently had a client with an Oracle database and several applications working through a WebLogic applications server. Oracle has a lot of great videos online touting the benefits of using their cloud services in such a case. Many helpful services are said to be bundled together to support the Oracle db/WebLogic combination.

Except that Oracle is cancelling the

service. Its new cloud services will not support it, and current instances will be phased out over the next few years. The only way we found this out was after a couple of weeks arranging a meeting with Oracle, because we had detailed questions. When we finally found the right people at Oracle and scheduled the right meeting, we found out that the main reason we were planning to go with Oracle no longer existed.

You can do more traditional hosting of WebLogic servers and make the system work in Oracle, much as you can in AWS and Azure. But Oracle's unique advantage for this option is on the way out.

What's a Newbie to Do?

So even hardened pros can be confounded when trying to get good information about cloud services. What hope do less experienced people have?

One thing I wouldn't try is googling "compare cloud services pricing," or something like that. You get these ambitious little comparison sites that somehow find some obscure product to be superior to the major vendors. Good luck with that.

Back in the day, before the Internet, I worked for Network Computing magazine. We had our own labs, or partnered with labs, to produce useful comparative product reviews. There were expensive, sort of the trade press's equivalent of investigative reporting. Now they are no more.


Some good comparative reviews exist. Idealware's comparison of products for nonprofits is excellent. You occasionally get a good one from what is left of the computer trade press, on the internet. Sometimes government sources, like NIST, come

also good that the phones will at least require a firmware update. Presume the worst and hope for the best here.

- Audio conferencing services. If you use Microsoft for your telephony "minutes" then you're all set. But if you use a third-party audio conferencing provider (example, PGI), you'll have to plan to transition away from that provider by July 31, 2021.

Where to Find the Details

Planning your Skype for Business Online transition can involve a lot of details. I could go into greater detail here. But Microsoft has done a smashing job pulling the information together, so I'll just point you there.

And if you need any help with this Skype for Business Online transition, you know who to call! 

Continued on Page 14

Comparing Cloud Services

Continued from Page 13

up with something useful. Sometimes a vendor will give you access to a report from Gartner, or another analyst, for free. But in general, doing good comparisons means a lot of time and hard work.

I sometimes even get so paranoid that I believe vendors are restricting information about their products on the web in order to get you to talk to a salesperson. More time spent and awkward situations ahead!

Something should be done.



Cybersecurity Safety Tips *by Dan Callahan*

I've been knee-deep in cybersecurity of late. I've been working on some handy cybersecurity safety tips, and thought I'd share them. As I work my way deeper into cybersecurity topics, I have to stop and remember that cybersecurity safety tips that might seem obvious aren't necessarily old news to everyone. So, let's review.

I've found that users are more engaged in cybersecurity training when you can offer them some cybersecurity safety tips that apply in their personal lives as well as at work. Let's start with a few of those tips.

E-Commerce Safety Tips

Let's start with an easy one: <https://> The key here is the s. It means secure. Any website you visit that is asking for money—say, a site for donations or a shopping site—should be using [https](https://). Look for it at the beginning of the URL in your browser's address bar. If you see <http://> instead (no "s") consider taking your business elsewhere.

And you probably know this, but think about your use of credit vs. debit cards. Credit card companies have a longstanding practice of suspending charges that are in dispute. You can get disputed debit card charges reversed, but sometimes it takes longer.

Think twice about storing your payment card information with an online retailer. Yes, it's much more convenient to store your payment information. But check and see if the online retailer has ever been hacked. Don't just presume that an e-commerce site will securely store your payment details.

After my checking account was hacked (for the second time), my bank suggested setting up a separate account just for debit card purchases and ATM transactions. Using a separate account this way has kept hackers from getting at my funds, as I keep these in other accounts.

Safety Tips for Social Media

Here are some social media tips, which also apply more broadly.

The best advice for securing your account identity is to use a strong password (or passphrase) and dual-factor authentication. Go here to learn more about that. However, many sites still use the "tell me a secret" authentication method (I made that up). These sites will ask you to answer a "security question" such as your mother's maiden name, the name of your first pet, etc.

This is one of those seemed-like-a-

good-idea-at-the-time ideas. After all, who would know these things? Well, depending on your level of social media sharing, a lot of people might know these things. So here's a cybersecurity safety tip: answer any of these questions with a nonsensical answer. For instance, when asked to name your first pet, answer "bagel" (unless you happened to have a cat named Bagel!) Even better, answer "bag3l". This will make correctly answering these security questions much more difficult for a hacker.

The simple cybersecurity safety tip in social media is this: don't connect with people you don't know. But even if you follow this practice, it can still be valuable to know how to spot a fake social media account. Here's a resource for that. And as the occurrence of image "deepfakes" grows, it's useful to know how to do a reverse image search. I tried this on an account that wants to follow me on Twitter and found the same image in several other (also fake) social media accounts.

My concluding cybersecurity safety tip is this: *exercise caution*. You don't have to be paranoid (unless you like being paranoid). But remember that people and things aren't always what they seem. 🕒

Tips for IT Strategic Assessments

Continued from Page 10

Translating the broad goals of the organization into specific initiatives can be a challenge. If you find somebody within the organization who can be clear on this, be grateful.

Often, despite documents full of missions and objectives, and despite a talk with the CEO, you still don't know the whole story. Talking to department heads is very important.

Your first point of contact, of course, are the people who hired you. Hopefully, these are the people who defined the project and who have been empowered to represent the organization to you. Good contacts are a joy to behold.

Spend enough time with them at the outset to define the research questions clearly. Draft some research questions and let your contacts revise them. You have your own ideas, and this is a good point to bring them up in the form of questions. Use the research questions to guide your creation of interview questions.

Interviewing

You can assess the current state of IT at an organization in many ways. I prefer gathering evidence from interviews. Interviews also uncover what people want.

Here are some don'ts about interviews: Don't do surveys. Written surveys are too impersonal, but don't even let your interviews behave like surveys. Please, not a long list of close-ended questions! But crucially, surveys make too many assumptions about what information you will get. The answers are too often determined by the questions.

I like guided, open-ended one-on-one interviews for managers and focus groups for the people in the trenches. Don't put managers and assistants to be in the same groups. Prepare different questions for each department, based on how they might see the overall issues from their angle. Let people go on, answering several questions with one answer and perhaps not getting to some issues.

Interviews as Therapy

Most people love to give their opinions. Sometimes, talking about IT in an organization is a bit like therapy, particularly if people don't feel they haven't had much of a say about IT. If you simply pay attention to people and bring out their thoughts, you will get a good interview. You will, of course, pick the topics for them to talk about, although the ones they bring up spontaneously sometimes turn out to be the most important. Don't try to show them how much you know or how clever you are. It just gets in the way of what you are trying to learn. Asking intelligent questions is enough.

Take good notes. It is so easy to forget important material. I've found that interviewees will tolerate my typing on a notebook computer during the interview. I've also found that telephone conversations can be as effective as face-to-face contact. With a microphone headset, this also gives you the opportunity to type.

The end of the interviews is a good time to write a needs assessment report. Submitting this for the client's review, and getting feedback, ensures you're on the same page. In general, both in this report and in the final report, good writing is essential. It needs to be clear, concise and a good read.

Project Management

In general it's good to have weekly project management meet-meetings with your official contacts in the organization. Do, however, let the clients make reasonable changes to this schedule. Their preferences are what matter, if meetings are still frequent enough to manage the project effectively.


Be sure always to keep to the schedule. There will be delays, but let them be caused by the client, not by you. The greatest source of delays will be scheduling the interviews. Many organizations we work with have people on the road more than half their time. Remember that phone interviews work and that you can talk to people on the road if they are comfortable with that.

The best tool for project management is a Gantt chart, or some other clear timeline, with the number of days and the dates for each task.

Some clients will have lots of delays. Tolerate this, but don't let it allow you to get lazy. If you can do work ahead of time, do it. If the delays begin to endanger the project, bring up the subject in meetings.

Are You Still Reading?

There's so much more to say about IT strategic assessments. We include security tests in our IT assessments such as vulnerability testing and evaluating threats to the organization's attack surface. IT policies have to be analyzed. We suggest technologies and often specific products. At the end, we put together a final report, a roadmap and very often a presentation.

So come back for more. There's so much more to do, and to avoid doing, that more posts will follow. 

A Message from the CEO

If I'm honest, one of the most fun things we do is produce content for our blogs. Selecting the content is the hardest part. We're looking for topics that folks will find useful and interesting, and for which we have experience and expertise. This year we have focused on security, new products, and ways that our user base can stay ahead of the game in terms of efficiency and effectiveness. Judging from the feedback we received, a lot of people are finding these useful and informative.

We tend to do about 2 articles a week, so it keeps Jackie, Dan and Tim busy. And when we hear exciting news from customers, we love publishing those stories as well! Each week we mail out a digest of the week's posts to our subscribers. Speaking of which, PLEASE SUBSCRIBE! Just go to cgnet.com and click on the red Subscribe button at the top.



Georg N. Lindsey

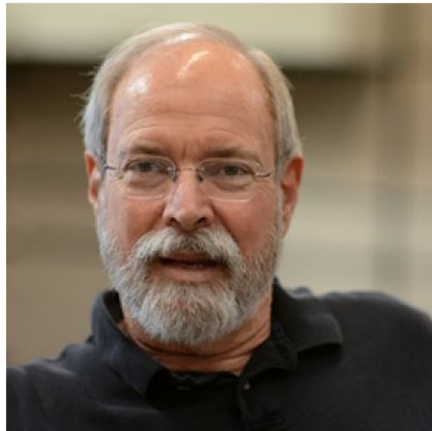


Meet the Bloggers



Dan Callahan

Dan is the VP of Global Services for CGNET. He is responsible for development of CGNET's cloud and cyber-security services. He oversees all aspects of CGNET's Office 365, Teams/Skype for Business, Azure, Enterprise Mobility + Security and Dynamics CRM Online cloud services. He is responsible for CGNET's vulnerability testing projects as well as GDPR compliance, risk assessment and security consulting services.



Tim Haight

Tim is the VP of Technology Services at CGNET. He has been studying how nonprofit organizations can optimize their use of information technology for more than 30 years, since he was the first evaluator for Apple Computer's Community Affairs Program. He has been at CGNET since 2002 and has conducted organizational analyses, assessments and strategic plans for a great number of CGNET customers.



Jackie Bilodeau

Jackie is the Communications Director for CGNET. She manages CGNET's external communication streams including website design and content, social media, newsletters, blogs, media campaigns and customer relationship management systems.

Contact Us

CGNET Services International
559 Clyde Avenue, Ste. 220
Mountain View, CA 94043
+1.650.833.6000