CSC

Cyber Security Toolkit

Defending against phishing, securing company assets, and creating robust passwords

CSC

Phishing

A major threat to businesses everywhere

What is phishing?

"Phishing is a criminal mechanism employing both social engineering and technical subterfuge to steal customers' personal identity data and financial account credentials."

- The total number of phishing attacks in 2016 was 1,220,523, a 65% increase over 2015.

- There's an average of 190,000 new malware samples found every day.

Phishing website: Which is fake?

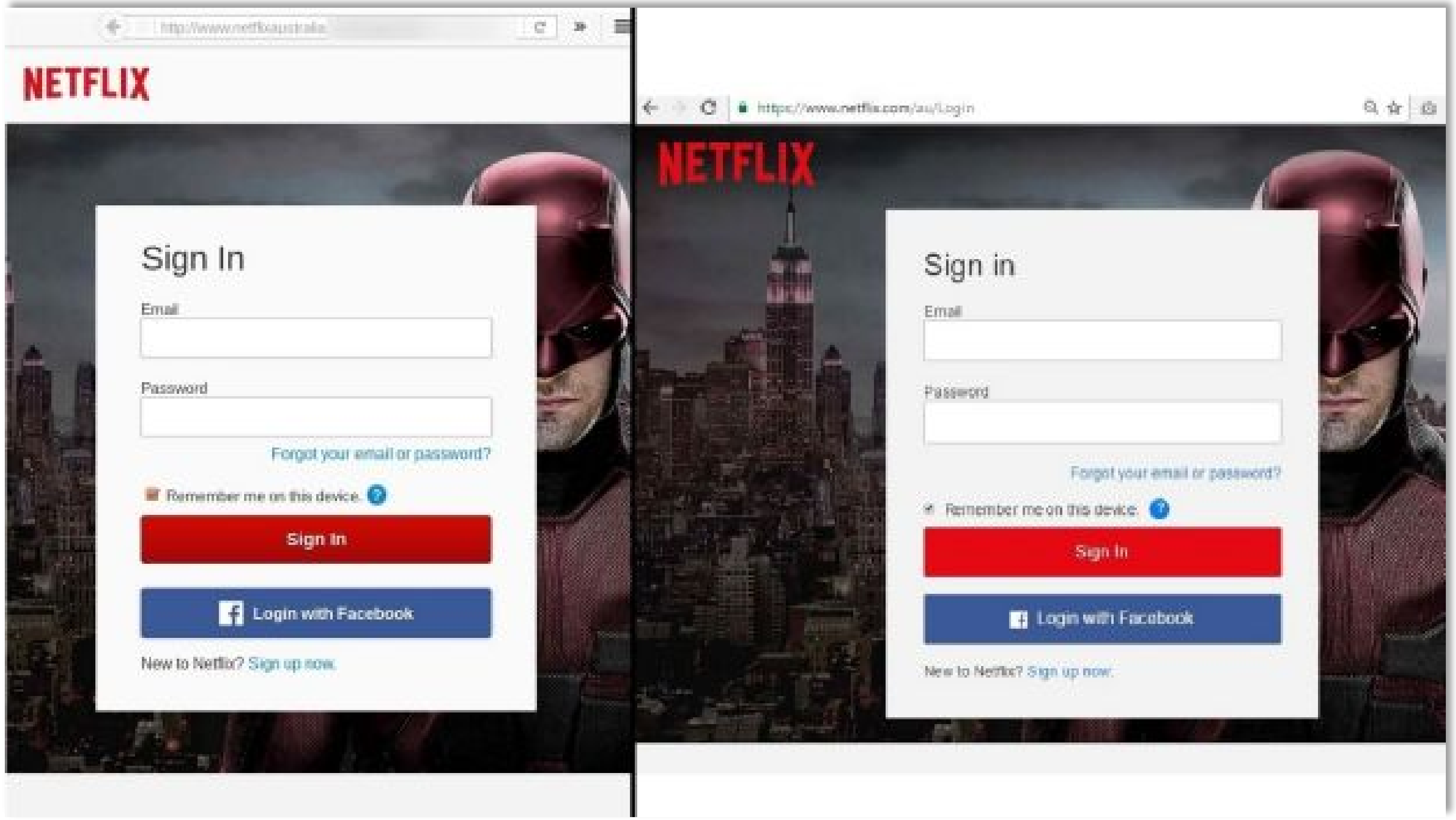

http://www.netflixaustralia
NETFLIX
Sign In
Email
Password
Forgot your email or password?
Remember me on this device.
Sign In
Login with Facebook
New to Netflix? Sign up now.
https://www.netflix.com/au/Login
NETFLIX
Sign in
Email
Password
Forgot your email or password?
Remember me on this device.
Sign In
Login with Facebook
New to Netflix? Sign up now.

Image source: http://www.theage.com.au/business/consumer-affairs/phishing-emails-and-other-online-scams-on-the-rise-as-australians-lose-millions-of-dollars-20161115-gspnar.html

Impact: The cost of a breach

48% of all breaches have been caused by malicious or criminal attacks.

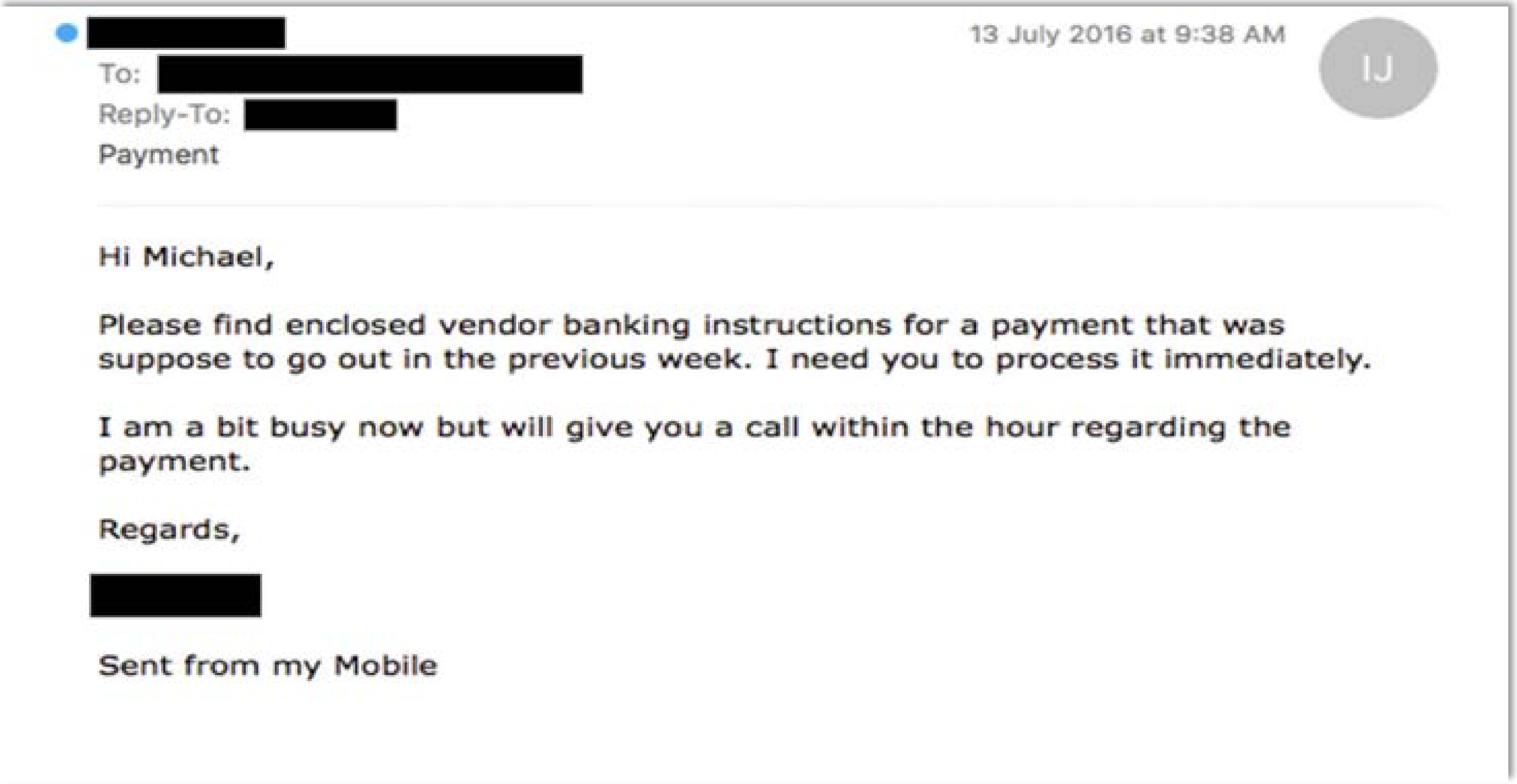
Phishing emails caused at least $3.1 billion in total losses around the world between 2013 and 2015.

How they work

- Cyber criminals use graphics, proper grammar, and key phrases that are similar to the spoofed brand.
- The messages they send evoke fear and urge immediate response.
- Cyber criminals spoof an authority figure to be more convincing.

Phishing attacks are more sophisticated, more pervasive, and more convincing than we think.

Example of an urgent email from an authority figure



[redacted]

13 July 2016 at 9:38 AM

To: [redacted]

Reply-To: [redacted]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[redacted]

Sent from my Mobile

Image source: http://www.mailguard.com.au/blog/whaling-ceo-fraud-business-email-compromise-targeted-spear-phishing-attacks-continue-to-trouble-businesses

Types of phishing: Email phishing

The biggest threat to companies right now is phishing, including spear phishing and CEO email fraud, which are email phishing attempts using a specific individual’s or company’s likeness.

- 30% of phishing emails are opened, and 12% of targets go on to click the link or attachment.
- 97% of people globally can’t correctly identify a sophisticated phishing email.

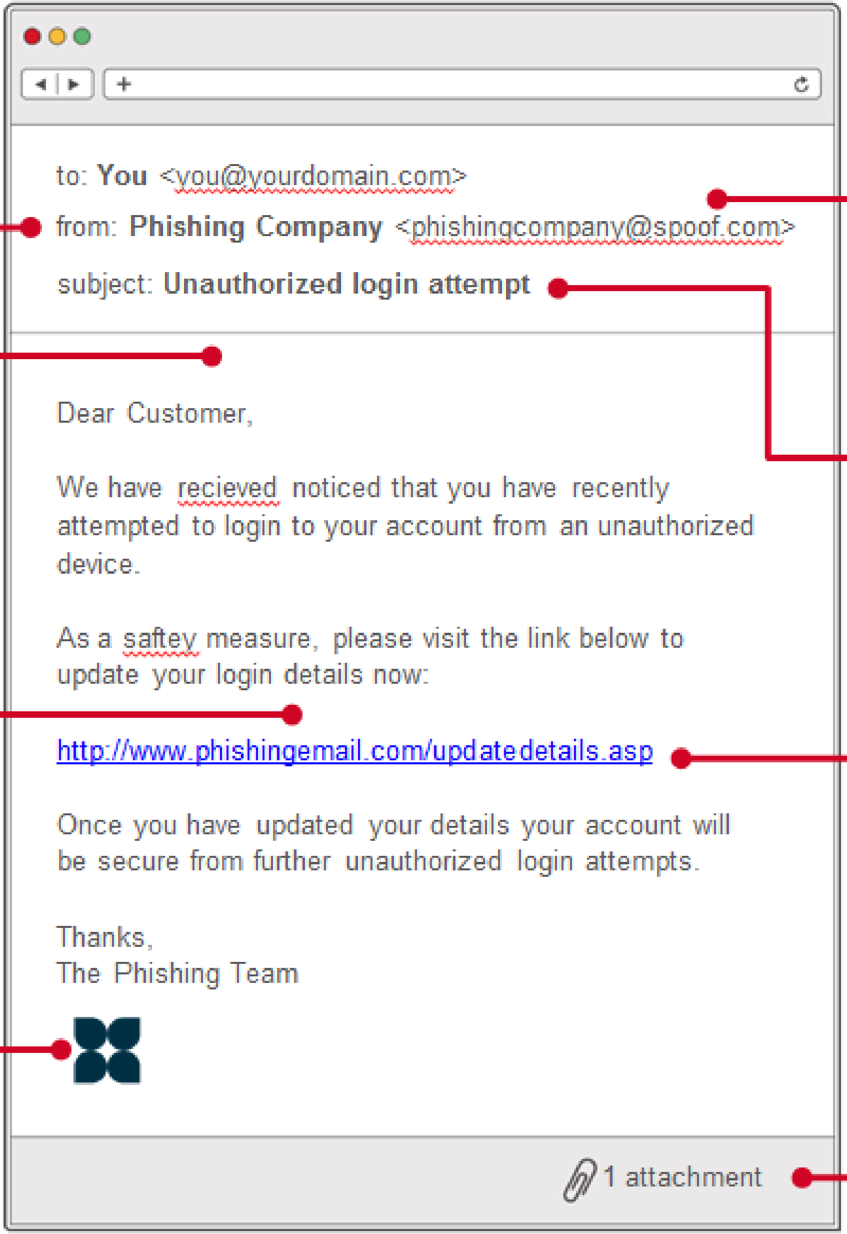
Types of phishing: Email phishing

Furthermore:

- Cyber criminals evolve their phishing email tactics to bypass spam filters.
- The availability of information on social media makes the research easy when creating a convincing phishing email.
- In an age when everyone is plugged in all the time on their smartphones, emails are accessed regularly, meaning phishing emails are read sooner, opening up another door of vulnerability for cyber criminals to get in—especially if an employee thinks they are receiving an urgent email from their CEO at 9 at night.

Anatomy of a phishing email

97% of people globally can’t correctly identify a sophisticated phishing email



to: **You** <you@yourdomain.com>

from: **Phishing Company** <phishingcompany@spoof.com>

subject: **Unauthorized login attempt**

Dear Customer,

We have recieved noticed that you have recently attempted to login to your account from an unauthorized device.

As a saftey measure, please visit the link below to update your login details now:

http://www.phishingemail.com/updatedetails.asp

Once you have updated your details your account will be secure from further unauthorized login attempts.

Thanks,
The Phishing Team

1 attachment

1 Making an email look legitimate by spoofing the company name in the “Display Name” field.

2 Tricking email servers into delivering the email to the inbox by spoofing the “envelope from” address hidden in the technical header of the email.

3 Including logos, company terms, and urgent language in the body of the email.

4 Making an email appear to come from a brand by using a legitimate company domain, or a domain that looks like it in the “from” field.

5 Creating convincing subject lines to drive recipients to open the message.

6 Including links to malicious websites that prompt users to give up credentials

7 Including attachments containing malicious content.

Top five email lures that get recipients to click

Verbatim from Proofpoint—a next-generation cyber security company

1. “Please see your invoice attached”

2. “Click here to open your scanned document”

3. “Your package has shipped”

4. “I want to place an order for the attached list”

5. “Please verify this transaction”

Email: Dos and Don’ts

- Be cautious with all attachments no matter who they are from. Especially those in suspicious formats like .zip, .exe.

- Mouse over links (without clicking) to verify they lead to the correct website URLs. Make sure it’s the website you intend to visit; this where you can see if the landing page for the link is really the brand you want to navigate to, or a spoof of that brand (which will include a bunch of unidentifiable words, letters, and characters). **When in doubt, don’t click.**

- When clicking “reply” to emails, always verify the email addresses of your recipients. You can also manually type them in, or insert them from an address book for the same reasons you want to check a website’s URL.

Email: Dos and Don’ts

- Use spam filters and updated protections. Updated anti-virus, anti-phishing, and email fraud protection solutions are basic forms of protection for you. Make sure these protections are updated regularly.

- When visiting websites, look for the green bar and the S at the end of HTTP. This is to check the site’s secure sockets layer certificates—the sign of a secure login for pages and forms where you may be inputting personally identifiable information.

Email: Dos and Don’ts

- If you don’t recognize the sender, be cautious with links and attachments. Even if you do know the sender, BE CAUTIOUS. Verify the contents of the email with a phone call to the person, or contact the company directly—especially if anything seems suspicious.

- Never respond to emails requesting personal identification or access information, especially if the request sounds urgent. Even if this request is from your CEO or CFO. Even if you are someone with whom the c-suite communicates with regularly. There is no harm in checking with that person first by phone or in person.

Email: Dos and Don'ts

- Do not click on popup windows that may redirect you to a fraudulent site or download malware.

- Be cautious of Live Chat windows, too, especially if they are asking for personal credentials.

Types of phishing: Telephone

Also known as voice phishing, or “vishing,” a phone call can be used to solicit personal information.

Caller ID can be spoofed and complex automated phone systems are used to make people believe the call is from your bank—about your credit card or banking activity—and it’s an emergency!!!

Text messages (SMS phishing, or “smishing,”) that usually contains an immediate call-to-action like a link to click or a number to call to “confirm” your personal information may also be used. If you click or call, malware that steals passwords could be installed on your phone.

Telephone: Dos and Don'ts

- Always verify the identity of the caller. If you answer, ask for a call-back number and their phone extension, or request a piece of information they should have on file for you.

- Research the Internet for reports from the same number. Unfamiliar caller ID formats or country codes may indicate a voice-over IP call or text message from automated systems.

- Look up the organization's customer service number. Rather than call the number given in the phone call or the text message, confirm the correct number by looking at your credit card, bank statement, or as a last resort, online.

Telephone: Dos and Don'ts

- Never respond to smishing messages. And never click on links, especially shortened ones that do not reveal their destination.

- Never reveal your personal banking details. Keep your PIN and CVV numbers private; the banks will never request such information because it's already on file for your account.

Types of phishing: Social media

Social media has few security controls, making it easy—and free—for cyber criminals to set up fraudulent accounts imitating real companies complete with authentic-looking logos, content, offers, etc. The criminals also sometimes pretend to be an employee of this imitated company, with a linked account to the actual company, to gain the user's trust in a social environment.

- 1 in 5 phishing attempts are now made through social media.
- A social media tweet for help to *@customerservice* can easily be intercepted by a response from *@customer-service*.

Social media: Dos and Don’ts

- Be mindful of social media comments and responses to your inquiries. They may come from fraudulent accounts. Instead, use official channels to reach out to a company.

- Be careful of websites and applications to which you link social profiles.

Social media: Dos and Don'ts

- Don't simply add unverified contacts to social media accounts, even if they claim to be from your company. And be wary of adding strangers, like recruiters, until you do your homework on them.

- Don't click on links from untrusted sources. Many social channels use shortened links that mask the real URL; the link could be spam or malware.

- Don't respond to suspicious email or messages. Even if it comes from friends, if it seems suspicious or out of character, their account most likely has been hacked. Inform them immediately by other means.

- Never share confidential and financial information. Even if conversations feel private, don't share confidential information on social media, not even photos that may include account statements or bills.

CSC

Securing Company Assets

Reducing inherent risks

A mobile workforce

- Nearly ¾ of the total U.S. workforce is expected to be mobile by the year 2020.
- 12.1 billion mobile devices are expected to be in use by 2018.
- Gartner predicts that by the end of 2017, over half of the globe's employers will require employees to "bring your own device" (BYOD).
- The most popular apps downloaded on employee devices are email, calendar, and contact management (84%), followed by document and editing apps (45%), then intranet (43%).

Inherent security risks

With constant connection comes inherent risks:

- 1 in 5 organizations in an information security survey suffered a breach of security due to employee mobile devices primarily connecting to malware downloads and malicious WiFi[2].
- 39% of surveyed organizations reported that BYOD or corporate-owned devices have downloaded malware at some point in the past[2].
- The average employee has more than 2 devices on them at all times, and few still use the Ethernet to connect, making WiFi a must[3].
- A high percentage of WiFi hotspots are using outdated security or no security[4].

CSC

Mobile: Dos and Don’ts

- Visit secured sites—check for the HTTPS in the URL, a green URL, and encryption lock—and minimize making financial transactions on public networks.
- Use a virtual private network to encrypt your online traffic, especially when connecting to a company network.
- Secure your device with strong passwords.
- Enable two-factor authentication for added security.

Mobile: Dos and Don’ts

- Keep software up-to-date with security patches, anti-virus protection, spam blockers, and spyware detection.

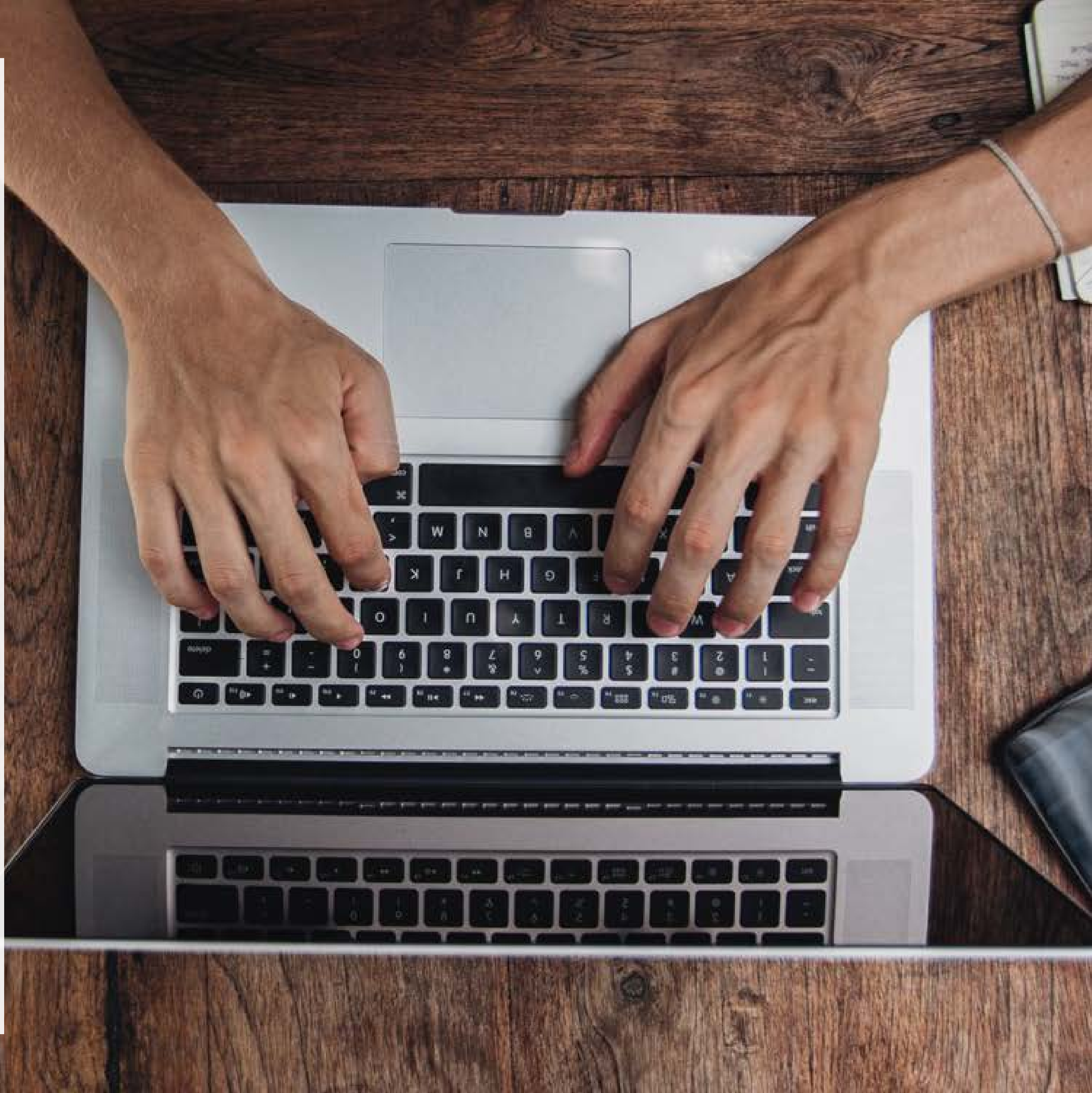
- Be mindful of phishing scams and malware links when checking email.

- When pairing your Bluetooth® unit to your phone or laptop, ensure that you are not in a public area where your personal identification number (or PIN) can be compromised, and switch the Bluetooth device to use the hidden (non-discoverable) mode.

Mobile: Dos and Don’ts

- Don’t connect to unsecured open WiFi hotspots (check for password-protection as one indicator of encryption being enabled).

- Don’t download programs or applications that you do not trust.



Password Security

The last line of defense

The importance of password security

A good password is free and an easy way to protect yourself from data breaches.

- 80% of analyzed data breaches are confirmed to be for financial gain

- 63% of breaches involved default, weak, or stolen passwords.

Compromised passwords

Passwords can be thought of as the last line of defense before a cyber criminal gets their hands on your data. Passwords can be compromised by:

- Fraudsters phishing for an individual's details, like username and password credentials, online banking information, and more.
- Brute-force attack by hackers who systematically compute all possible passphrases and patterns.
- A data breach on a company or website that has been hacked, resulting in millions of compromised accounts.

Common failings in passwords

Before and after a data breach, a complex password is the most secure.

Make it something you can remember, but with a twist that a cyber criminal wouldn't be able to figure out—so that means you shouldn't use your dog's name! Here's some common password failings you should avoid:

- The top 3 most popular passwords are *Password1*, *Welcome1*, and *P@ssword*.
- The most common keywords used in passwords include baby, pet, and city names.
- Close to 30% of the top 10 character sequences are in this format: Uppercase letter (U) followed by a series of lowercase letters (l) appended by numbers (#) at the end such as *Ulllll##*, for example *Hello11*.

Password: Dos and Don'ts

- Complexity is important but password length is the key. Using long passwords (at least 10-characters) makes it harder for cyber criminals to decode them.

- 8-character passwords are cracked within 1 day using brute-force techniques; 10-character passwords require about 591 days—close to 600 times more effort! Use collections of words that form a phrase or sentence you can remember, but is random to anyone else, such as *TW2gsi2QT&bd* = quote by Walt Disney "The way to get started is to quit talking and begin doing." Always use a master password and a password manager.

- Beyond secure passwords, two-factor authentication can help restrict compromises. Attackers will move on to an easier target instead of spending effort to compromise both modes of authentication.

Password: Dos and Don’ts

- Avoid using predictable patterns like *Ulllll##,* or adjacent keys like “*qwerty*” and “*asdf*.”

- Don’t use dictionary words in your password, or family members’ and pets’ names, addresses, or confidential details like identification numbers, birth dates, social security numbers, or phone numbers.

- Don’t use the same password for multiple sites. A data breach on any account would render even the most complex password useless if it was re-used on multiple accounts. Never use the password for your email account at any online site.

- Don’t store your passwords in plain text on any computer.

CSC℠

CSC

Thank You!