Metal Sales™

IT Security Awareness Training

6-2025

WHY IS IT SECURITY IMPORTANT AT METAL SALES?

1. We rely heavily on our IT systems which must always be available to conduct company business, serve our customers and support our employees.
2. We are responsible for Metal Sales data accuracy & integrity and for preventing unauthorized changes & access (e.g. pricing, inventory records).
3. A strong IT Security awareness allows us to collectively minimize the risk of business disruption caused by successful cyber attacks.

Each one of us plays an important part in successful cybersecurity risk management!

Metal Sales

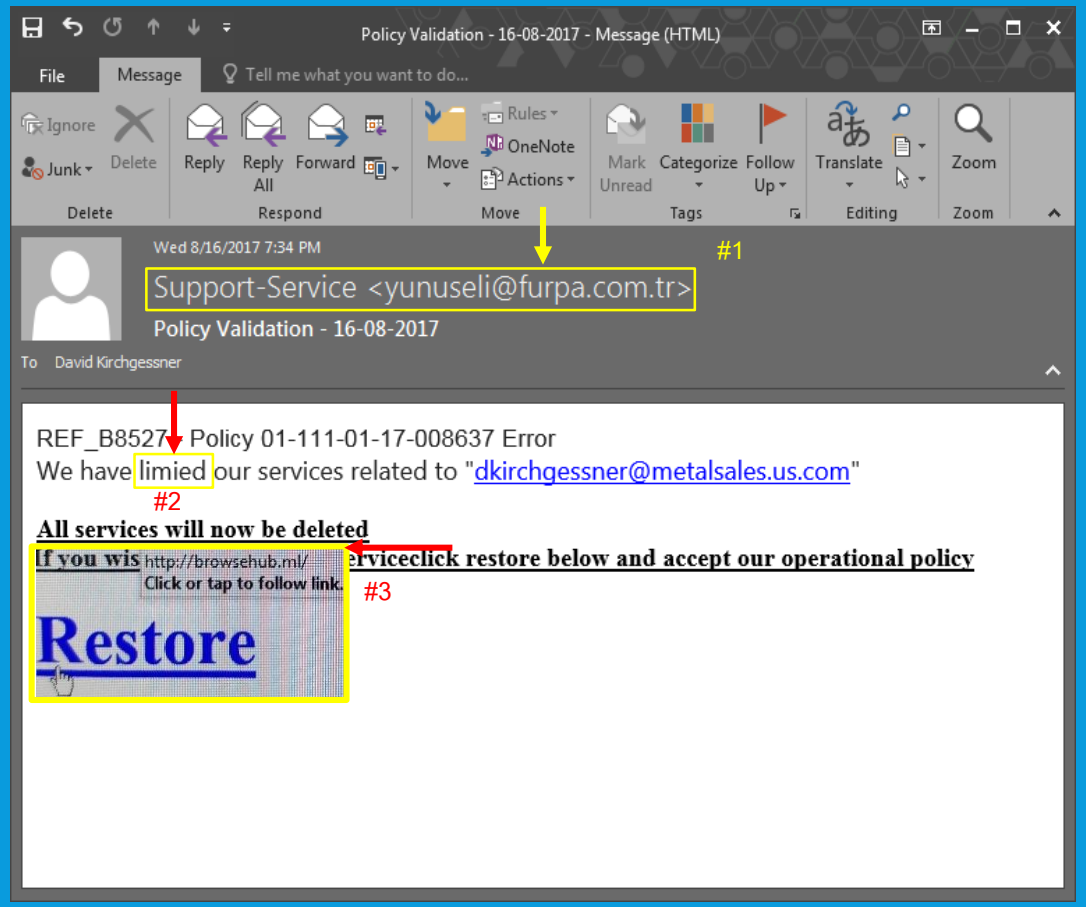
THREAT TYPE 1: "PHISHING"
LOOKING FOR INFORMATION ABOUT METAL SALES OR YOURSELF

- Phishing is the number one way that “attackers” attempt to gather information about a company or specific employees.
- Email is one of the primary tools used to try to get this information.
- Phishing emails may appear to have come from someone within the company, a customer, or a vendor that you communicate with regularly.
- It may also contain a link to a website that will trigger a malicious file download, infecting your computer with malware or a virus.
- Some emails may also contain attachments; for example, a fake invoice or something similar. These files can contain malware or viruses as well, that activate when you open the attachment.

Metal Sales™

THREAT TYPE 1: "PHISHING"
EXAMPLE

- Here is an example of a Phishing email
- Note the sender FULL email address ending in .tr which means this is from Turkey (#1) even though the display name is “Support-Service” which may seem legitimate at first glance.
- Other indicators of malicious emails are poor grammar or misspelled words as attackers are often not native English speakers. (#2)
- Finally, be wary of any links to websites. The word Restore in this example is a link to a website with the address: **http://browsehub.ml.** The website address ends in .ml, which means it is from Mali. (#3)
- If you have any doubts or questions, contact the Helpdesk via phone (x4315) or submitting a ticket at https://helpdesk.metalsales.us.com



Metal Sales

THREAT TYPE 1: "PHISHING"
BE CAUTIOUS OF SUSPICIOUS EMAILS AND LINKS

- In addition to company & employee information, hackers may try to steal mailing lists, which happened recently to Toshiba.
    - A webserver was hacked and personal data (email addresses, phone numbers and passwords) relating to 7520 customers was compromised.
- Always delete suspicious emails from people you don't know. And never click on the links. If you are unsure an email is legitimate, contact IT and we can help you determine if the email is safe or not.
- Opening these emails or clicking on links in them can compromise your computer without you ever knowing it (anti-virus programs do NOT catch everything).

Metal Sales™

THREAT TYPE 2: SOCIAL ENGINEERING
VIA EMAIL, PHONE OR IN PERSON

- Social Engineering is another way for the “bad guys” to attempt to get information to use in gaining access to company resources (i.e. computers, financial information, physical access to a building, etc.)
- Someone calling and pretending to be from the Metal Sales Helpdesk or IT and asking you for your username and/or password so they can fix a problem you didn’t even know you were having, could be an attempt at Social Engineering.
- An example of Social Engineering via email could be: receiving an email that appears to be from an address like “administrator” or “helpdesk”; the body of the email could ask you to “reset” your password or confirm it by responding to the email with your username and password.
- The IT department typically does not need your password to fix problems. We will ask you to key it in yourself, when we help you, if necessary.
- Another form of Social Engineering is “tailgating”. When someone tries to gain access to the building by coming in after you have scanned your security badge or asking if you can let them in because they forgot their badge at home. Be mindful of people you don’t recognize attempting this.

Metal Sales™

THREAT TYPE 2: SOCIAL ENGINEERING
DO NOT BE TRICKED INTO GIVING AWAY CONFIDENTIAL INFORMATION

- Do not respond to emails or phone calls requesting confidential company information or your personal information.
- Always keep in mind that “bad guys” are successful because they are convincing.
- Recent news stories out of Canada reported scammers were tricking people into giving away information with fake tech support calls claiming to help.
    - The scammers pretended to be from Microsoft, needing to remotely connect to the person’s computer to install (fake) anti-virus software or another program that was actually malware and then charge the person for their “assistance”.
- Stay alert and report any suspicious activity (including suspicious phone calls) to the Help Desk.

THREAT TYPE 2: SOCIAL ENGINEERING
NEVER MAKE PAYMENTS BASED ON AN EMAIL REQUEST ALONE

- Another classic Social Engineering trick is to send an email that may look like it is coming from a company executive requesting a wire transfer or some other form of electronic payment.
- ALWAYS verify the request by calling the alleged sender via a known good phone number for that person.
- ALWAYS get a second and different approval from management or Corporate Finance.

In 2016, The FBI estimated that email wire transfer requests scams have cost US organizations more than $2.3 billion in losses over the past three prior years.

Metal Sales™

THREAT TYPE 3: WEAK PASSWORDS

- Always use hard-to-guess passwords
- Many people use obvious passwords like “password,” “cat,” or obvious character sequences on the qwerty keyboard like “asdfg.”
- Create complex passwords by including different letter cases, numbers, and even punctuation.
- Use different passwords for different websites and computers:
  if one of your accounts gets hacked, and you use the same password everywhere, all your other accounts can be easily compromised as well.
- Do NOT write passwords down on Post-Its, etc.

THREAT TYPE 4: PHYSICAL SECURITY
ONLY USE METAL SALES COMPUTERS

- The Metal Sales IT Team keeps Metal Sales laptops & desktops up-to-date with regular systems and anti-virus updates.
- Personal or public (e.g. library, hotel lobbies) computers might not be maintained with the same standard of care, so they are unsuitable to access Corporate systems and data.
- One exception to this rule is your Metal Sales email which may be accessed via a personal mobile device (smart phone or tablet) when authorized by the Metal Sales IT Team.

NOTE: if you have a Metal Sales laptop, be sure to connect to the Metal Sales network at least once a month (do this using VPN if you rarely visit one of our facilities) to ensure your laptop receives all necessary updates (contact the IT Help Desk if you have questions about this).

Metal Sales

THREAT TYPE 4: PHYSICAL SECURITY
DO NOT LEAVE SENSITIVE INFORMATION LYING AROUND THE OFFICE

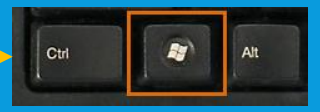
- Do not leave printouts containing sensitive information on your desk. It's easy for a visitor to glance at your desk and see sensitive documents. (i.e. financial documents, employee information, payroll information, etc.)
- Keep your desk tidy and documents locked away or shredded when no longer needed.
- These simple precautions reduce the risk of information leaks.

REMINDER: do NOT write your username and password down and then have them visible near your workstation.

Metal Sales™

THREAT TYPE 4: PHYSICAL SECURITY
LOCK COMPUTER AND MOBILE PHONE WHEN NOT IN USE

- Always lock your computer and mobile phone when you're not using them. You work on important things, and we want to make sure they stay safe and secure.
- Locking these devices keeps both your personal information and the company's data and contacts safe from prying eyes.



- You can easily lock your computer by pressing the windows key + L on the keyboard.
- If you need assistance with how to secure your computer or mobile devices, contact IT and we will gladly help you.

Metal Sales

THREAT TYPE 4: PHYSICAL SECURITY
DO NOT PLUG IN PERSONAL DEVICES WITHOUT IT APPROVAL

- Do not plug into your Metal Sales computer your personal devices such as USBs, MP3 players and smartphones without permission from IT.
- Even a seemingly harmless USB flash drive could be infected with a nasty virus.
  - The supermarket chain Aldi was reported to have sold pre-infected removable hard drives in stores and IBM gave away USB flash drives with viruses on them at a conference. These and other well known companies have unknowingly distributed infected devices to customers.
- These devices can be compromised with programs waiting to launch automatically as soon as you plug them into a computer.
- Contact the IT Help Desk if you believe you have a legitimate reason to want to plug a personal device in your Metal Sales computer.

Metal Sales

THREAT TYPE 5: SOFTWARE SECURITY
DO NOT INSTALL UNAUTHORIZED SOFTWARE PROGRAMS

- Do NOT install unauthorized programs on your work computer
- If you like an application and think it will be useful, contact the IT Help Desk and we'll look into it for you.
- Malicious applications often pose as legitimate programs like games, tools or even antivirus software.
- They aim to fool you into infecting your computer and spread across the network to other files or computers.
- This recommendation also applies to your personal mobile devices:
  - Install only applications you really need.
  - Only install apps from the Google Play Store or Apple iTunes Store.
  - Do NOT install apps from random websites or other third party applications providers.

Metal Sales

IT SECURITY THREAT TYPE SUMMARY

·Threat Type 1: Phishing

- Unsolicited emails that may appear to come from reliable sources containing links to websites and/or questionable attachments (e.g. fake invoice or package delivery notice) and/or requesting personal/confidential information. Contact Metal Sales IT Helpdesk if you are unsure. x4315

·Threat Type 2: Social Engineering

- Receiving a phone call from someone pretending to be from Metal Sales IT, customer, or vendor that requests access to your computer or personal/ confidential information. This can also be a person that is trying to enter the building claiming to be an employee or contractor.

·Threat Type 3: Weak Passwords

- Easily guessed passwords (i.e. password, 123456, etc.). Create complex passwords using different letter cases, numbers and even punctuation. Also, try to use different passwords for different websites and computers so if one account is hacked, the others are still safe.

·Threat Type 4: Physical Security

- Lock you computer, cell phone, or tablet when walking away from them. Do not leave sensitive documents laying around your desk that someone could walk by and read or take. Do not connect personal devices (USB drives, phones, etc.) to Metal Sales computers without getting the Ok from IT dept.

·Threat Type 5: Software Security

- Do not install unauthorized programs on your work computer. If you like an application and think it will be useful, contact the Helpdesk and we'll look into it for you. Malicious applications often pose as harmless programs like games, tools, or even anti-virus programs. This also applies to your mobile devices. Installing apps from websites or other third party providers, instead of from the Google Play Store or Apple iTunes Store can infect your mobile device with malware or a virus rendering the device unusable or comprising your personal information.

Metal Sales™

Metal Sales™

Remember:

- IT Security is only as strong as its weakest link.
- We all have a part of responsibility in this area.

Thank you for doing your share by following these guidelines to help safeguard Metal Sales network, data and devices and ultimately protect our business.